NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

THESIS

INTERNET AT SEA FOR THE HELLENIC NAVY

by

Panagiotis Lymberis

March, 1997

Thesis Advisor: Rex Buddenberg

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.		
1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 1997	3. REPORT TYPE AND DATES COVERED Master's Thesis
4. TITLE AND SUBTITLE INTERNET AT SEA FOR THE HELLENIC NAVY		5. FUNDING NUMBERS
6. AUTHOR(S) Lymberis Panagiotis		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey CA 93943-5000		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSORING/MONITORING AGENCY REPORT NUMBER
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.		
12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.		12b. DISTRIBUTION CODE

13. ABSTRACT

The Hellenic Navy is confronted with a set of mission-related challenges that can not be efficiently supported by existing information systems. However, the transition to more modern information systems needs to fulfill a basic principle of command and control, "unity of purpose". This thesis uses the unifying concept of information architectures to identify some desired characteristics for future HN information systems. Two real-life projects are reviewed to substantiate the analytical suggestions borrowed by the client-network, or network-centric architectural paradigm. The "SeaNet" project is used to show the feasibility and utility of extending internet technologies to the maritime environment. The "Battle Force e-mail" project is presented as a pilot program for the introduction of TCP/IP based data exchange between units at sea. At the concluding Chapter, a set of recommendations is made for the transition to a network-centric information architecture for the Hellenic Navy and the development of internetworking capabilities over seawater.

14. SUBJECT TERMS Internet, information architecture, data communications, hellenic navy			15. NUMBER OF PAGES 124
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18 298-102

Approved for public release; distribution is unlimited.

INTERNET AT SEA FOR THE HELLENIC NAVY

Panagiotis Lymberis
Lieutenant, Hellenic Navy
B.S., Hellenic Naval Academy, 1986

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 1997

Author: ______________________________
Panagiotis Lymberis

Approved by: ______________________________
Rex Buddenberg, Thesis Advisor

____
Suresh Sridhar, Second Reader

Reuben T Harris
____
Reuben T. Harris, Chairman
Department of Systems Management

ABSTRACT

The Hellenic Navy is confronted with a set of mission-related challenges that can not be efficiently supported by existing information systems. However, the transition to more modern information systems needs to fulfill a basic principle of command and control, "unity of purpose". This thesis uses the unifying concept of information architectures to identify some desired characteristics for future HN information systems. Two real-life projects are reviewed to substantiate the analytical suggestions borrowed by the client-network, or network-centric architectural paradigm. The "SeaNet" project is used to show the feasibility and utility of extending internet technologies to the maritime environment. The "Battle Force e-mail" project is presented as a pilot program for the introduction of TCP/IP based data exchange between units at sea. At the concluding Chapter, a set of recommendations is made for the transition to a network-centric information architecture for the Hellenic Navy and the development of internetworking capabilities over seawater.

TABLE OF CONTENTS

I. INTRODUCTION

A. C4I AND INFORMATION ARCHITECTURES

1. Definitions

The Hellenic Armed Forces are considering a multi-billion dollar arms procurement bill, to meet short-term Greek defense needs[1]. At the same time, military organizations worldwide are coping with the implications of the information technology related and much publicized "revolution in military affairs." (Cohen, 1996) This thesis argues that the Hellenic Navy, by using its appropriated portion of the bill, should invest on a new information architecture to meet current and future tasks. This new information architecture could become the framework that will provide the "competitive advantage" for a relatively small navy --which many times extends its available resources to the limit-- to accomplish its tasks. Two ongoing real-life projects are used to illustrate different aspects of a model architecture. To acquaint the reader with some of the concepts used in this work a background section is deemed appropriate in this introductory chapter.

Information is the critical component in decision-making processes, at any level. "Military organizations have traditionally provided information to forces in three ways: commands, intelligence and doctrines." (NDU, 1996) The lack of complete information in warfare has led to aphorisms such as "the fog of war." It is essential therefore, for any

[1] From Greek Defense Policy at: http://www.mod.gr/greek/politiki.html (21 February 1997)

maritime force to exploit all available information in the most efficient way. Perhaps we could better understand information by saying what it is not and what are its desired attributes. Information is not data. It is data processed into a usable form. To be useful it has to be accessible, relevant, comprehensive, timely, accurate and secure (Wolstenholme et. al., 1993, Joint Pub 6-0, 1995). Information value accrues as it relates to individual or organizational needs. (Grenier and Metes, 1992) Expanding on the concepts above, information has to be traceable and extractable. It has to be focused on the task that it supports to avoid information overload on the decision-makers. It has to be presented in a format acceptable to the decision-maker, so that format-related ambiguities are minimized. In addition, it has to be received and processed as long as it is relevant to the situation at hands. Timeliness of information though, has always been in contrast with its accuracy. Communicators around the world have been struggling with the impossibility of achieving optimal reliability, speed and security at the same time. Security of information involves issues such as the need for encryption, authentication and other forms of protection.

Information technology is "an all inclusive term that encompasses computers and telecommunications in all their forms, whatever their use." (Hoffman, 1994) It can be argued that information technology at a conceptual level predates the computer. The dissemination of the news about Troy's sacking by Greeks around 2000 BC, exploited information technology of the time. Huge fires on mountaintops (routers) ensured with acknowledgment (seeing the next fire), the transmission of the campaign's end (information) from the remote expedition force (sensor, weapon) to the mainland (support center). Yet, a more inclusive term --information systems-- has been used to relate

information technologies to business processes. *Information system* "is a combination of information technology and other things which usually include business procedures, paper forms and human effort, organized to support or manage a business process." (Hoffman, 1994) The distinction between information technology and information systems is based on the inclusion of non-technological parts in information systems. This allows different "organizing methods" of the same technology to create systems of varying efficiency in supporting business processes. For the navy, one of the most basic processes is the exercise of command and control of forces. In a formal definition C2 is:

> The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (Joint Pub 6-0, 1995)

It is interesting to note the complementarity between information systems and the above definition of C2. As is the case with information systems, C2 also aims to support "a mission." In Table 1, the tasks of command and control are listed. It is difficult to imagine today completing those tasks without some use of information systems.

Command is the art of:	*Control is the science of:*
Visualizing a future state	Computing requirements
Formulating concepts of operations	Allocating means
Prioritizing and risk assessment	Applying means to accomplish commanders interest
Assigning missions	Developing specific instructions
Selecting critical time and place	Describing interfaces
Anticipating change	Measuring, reporting and analyzing performance
Seeing, hearing and understanding	Project change
Decision making	Identifying variance
Leading, guiding and motivating	Correcting deviations

Table 1. Command and control tasks (After NDU, 1996)

However, there is a clear hierarchical distinction between the end, which is command and control and the means which include information systems as one of them (see also below the discussion on information architectures).

Advances in information technologies effect the following characteristics of an information system: reach; range; depth; and change. (Hoffman, 1994) Reach expresses the spatial and user extent of an information system. Range represents the vertical sharing of information within a system or the horizontal distribution across systems, organizational boundaries and hierarchies. Depth refers to the extent information permeates business processes. Change is the capability an information system has to adapt to technological or environmental (in the broad sense) changes. While we can satisfy our needs in the first three, at an associated premium, change has been the most difficult to harness. As systems develop from having little depth, low interaction and a limited number of users, to being highly information dependent systems of high interaction and reach, change can take many different paths. Change has become the starting point of this thesis, by attempting to define and manage the required transition in information systems for the HN. The development of information technologies requires a continuous examination of information systems for the achievement of a "best fit" among mission needs, organizational structure and available technologies.

In a C4I environment, IS complete the tasks of acquiring data about the environment, fusing data to create information, transporting data and information to decision makers and providing the communications means to disseminate and implement decisions (Buddenberg, 1995). In an abstracted form, C2 as seen from an information systems perspective would look like Figure 1.

Information architecture is an analytical tool for organizing information systems. The paradigm of architecture draws from the construction world the concept of detailed design and structure. Hoffman defines information architecture as "the set of design criteria, implementation rules, and technical standards that governs the design, deployment and operation of all information technology and systems in an organization." (Hoffman, 1994) Information architecture, nonetheless, is a constraining paradigm since it evokes strict rules to be followed in the "construction" of a system. Today's military organizations, following business paradigms, seem to opt for less hierarchical and more flexible structures in their commands. (Hazlett, 1996) Therefore, past information architectures such as mainframe, personal computing, distributed computing or even client/server do not seem adequate or appropriate for dynamic complex organizations.

One proposed solution is client-network computing (Lippis, 1997) or what Hoffman terms as a*pplication -infrastructure architecture* (Hoffman, 1994) Information systems are categorized in those which support unique applications (vertical information systems) and those which support many applications --infrastructure-- (horizontal information systems). Components of the infrastructure are the computer and communications networks, data, technical tools and administrative procedures, as well as the people and the organization. Buddenberg has proposed a similar concept specially for military organizations and emergency services, "the network centric vision." (Buddenberg, 1995) Instead of focusing on the details of the end nodes of an information system (application specific), we could focus, he proposes, on the network-infrastructure substrate that support them.

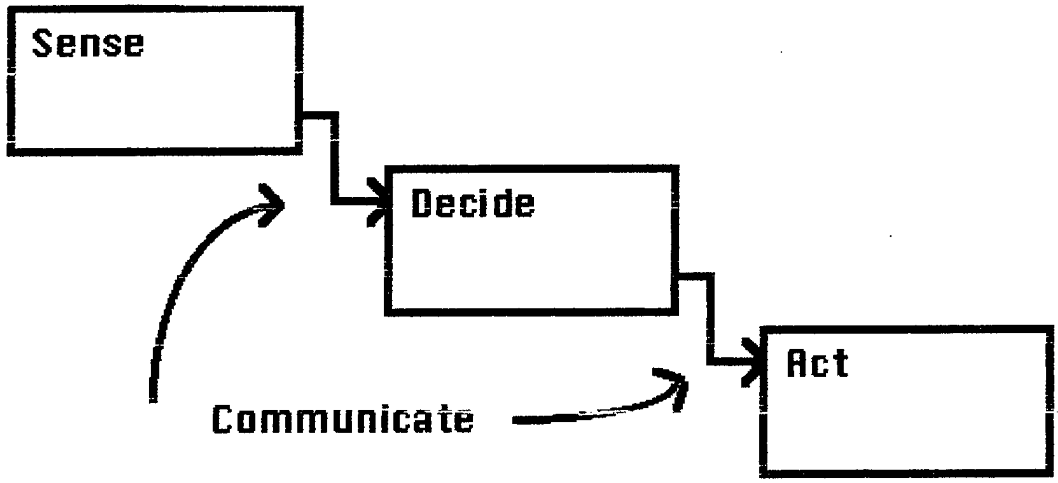


Figure 1. Generalized model of an information system (From Buddenberg, 1993)

The benefits of concentrating on the "cohesive" infrastructure instead of focusing on individual systems are:

- The network-infrastructure can be shared by several systems with direct implications in survivability, availability and affordability.
- Incremental development of the network is made possible by the support for orderly deployment of new systems. Our attention is on the interface of the system with the infrastructure through open standards.
- Economies of scale can be obtained by sharing resources across the network.
- Upgrade and replacement of end systems is easier since it can be accomplished without affecting the integrity of the whole architecture. (Buddenberg, 1995, Hoffman, 1994)

A conceptual view of such an architecture is Figure 2.

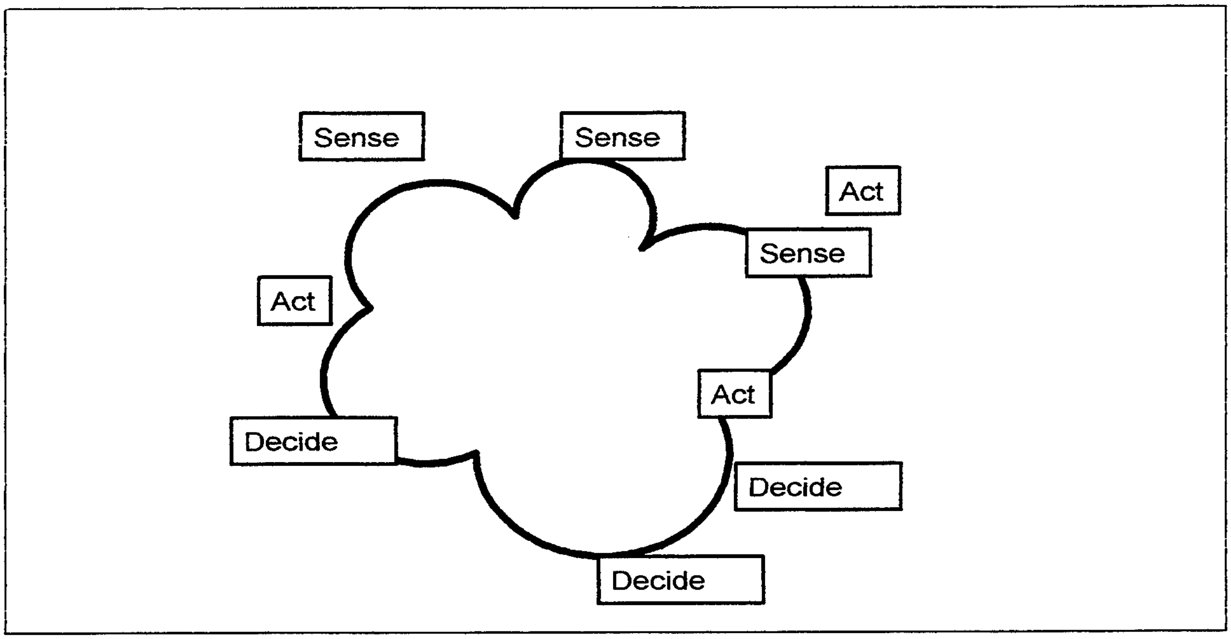


Figure 2. Network-infrastructure cloud with C2 functions (From Buddenberg, 1993)

Focusing on the communications aspect of architectures we can differentiate between infrastructure and applications by structuring the levels of services provided in layers. Figure 3 shows a telecommunications model architecture with the various provided services and examples. The analogy with the Open Systems Interconnection model is obvious. At the lowest layer, we identify the physical links and their parameters which provide the necessary bandwidth for communications needs. At the next higher layer, routing services among information users are provided. Value added services in the third layer include basic services to users. E-mail capability, capability for the exchange of information system management, time synchronization and directory services are good examples. The highest layer of information services includes the application specific systems such as weapons, sensors or management agents.

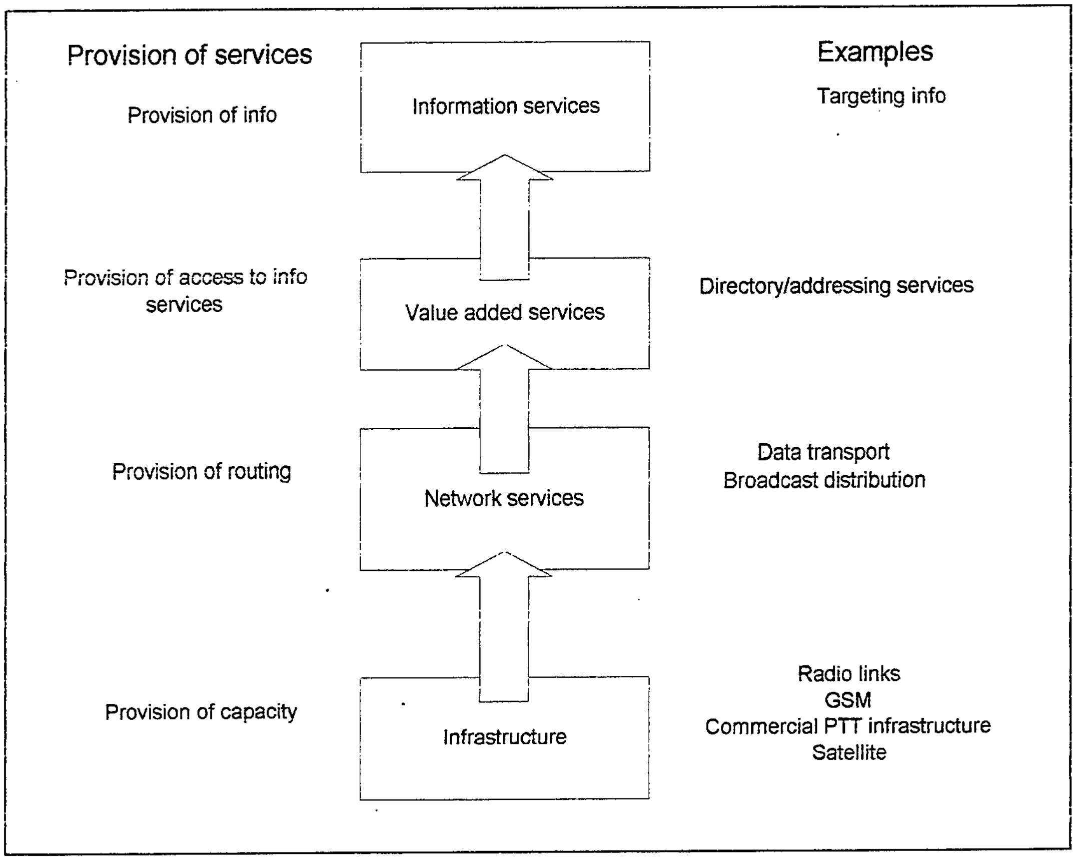


Figure 3. Layered model for telecommunications (After Kahin and Wilson, 1997)

Information architectures allow us to differentiate between the constant elements in our strategic planning such as vision and long-term objectives (infrastructure) and the changing tactics we use to cope with immediate needs (application, end nodes). The HN faces today challenges in both realms, which make the need to review and modernize its information systems imperative.

2. Challenges for the Hellenic Navy

Anticipated changes in missions, an armed forces-wide initiative emphasizing joint structures, advances in information technologies and economy considerations, constitute the major challenges HN has been facing the last years. Those challenges have direct consequences for the information system the HN uses or plans to deploy. Mission oriented challenges stem from the potential extent of the area of interest for HN commanders well beyond the confines of the Aegean Sea; the variety of conflict levels (peacetime, operations other than war, crisis, conventional war) it expects to be drawn into; the incessant need for reliable, real-time and secure exchange of information among units and commands at sea and the various command centers at home; and the requirement for interoperability with multinational forces such as future NATO or WEU CJT (command joint task) forces. The Navy's role in assisting the Hellenic Coast Guard in operations other than war (anti-drug trafficking, anti-smuggling, border patrols) also requires intensive use of C4I resources.

The area of interest for HN poses a hard requirement on information systems. The GSM cellular infrastructure is a physical link that merits examination for operations near the coast. However, the support of open sea operations has to rely on HF and satellite-based links as the long-haul information pipes.

The variety of conflict levels "impose different and sometimes contentious requirements on the C4 systems that support them." (Joint Pub 6-0, 1995) In peacetime, and bearing in mind that HN aims to deter, three main missions need to be supported:

- Routine operations
- Attack warning and
- Transition to war

Those missions imply tasks that need scalable information systems, capable of providing timely, secure information across the area of operations. In crisis situations, information systems have to provide for immediate and extended connectivity among theater forces and decision-making centers, afloat or at home. The requirements of crisis management impose heavy loads on the information infrastructure. Conventional war requires the capability to reconfigure and reconstruct networks and systems as the underlying topologies, either physical or functional, change. In operations other than war, information systems are expected to integrate or at least, connect to the existing civilian infrastructure, be easily deployable and re-configurable.

Organization related challenges arise from emerging joint structures within the Hellenic Armed Forces, especially in areas such as intelligence and "battlefield" picture compilation and exploitation. The need to train personnel in new technologies and the establishment of appropriate policies for their use creates issues that have to be addressed *a priori*. Moreover, economic considerations push for greater savings, reliability and interoperability of individual information systems.

Advances in information technologies affect the way any military organization conducts operations. Figure 4 shows the potential extent of the impact new information technologies will have on doctrine, C2 and capabilities. Cohen argues --at a different level -- that the most important implications on military organizations will be on the way wars are fought, on the structure of the military organizations, on civil-military relations

and on the overall power assessment for a specific country.(Cohen, 1996) The scope of the thesis is not as broad as to include such issues. However, it is necessary to understand the potential implications of information technology advances, in order to better manage their deployment in real systems.

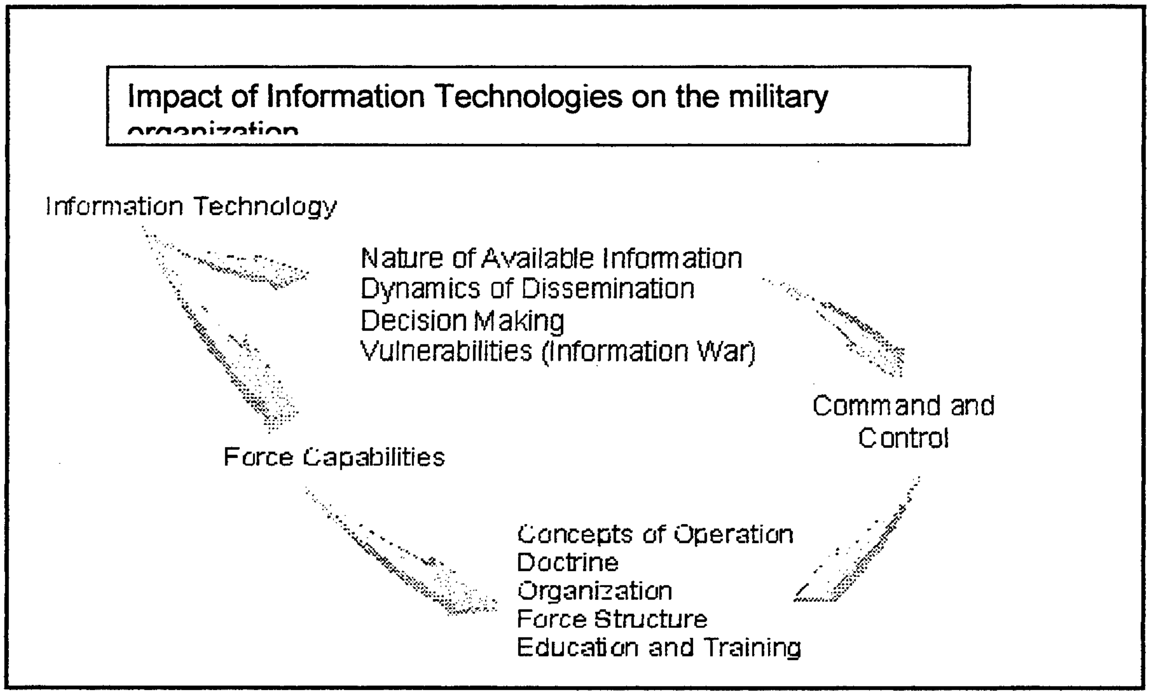


Figure 4. Impact of information technologies on the military organization (NDU, 1996)

B. PROBLEM DEFINITION

1. Current infrastructure

The problem for the HN is twofold: how to identify requirements for needed information systems and how to manage the transition from the *status quo* to the desired end state. Before embarking on any of those questions, an inventory of information

systems already in place is necessary. A brief review reveals a multitude of stovepipe systems not exchanging information with each other. Furthermore, information is "pushed" to the users, as they have limited interaction capabilities with data repositories.

For exercising command and control of forces at sea, HN relies mainly on HF teletype communications and voice circuits, along with some satellite communications. Tactical systems such as Link1, Link 11 and Link 14, are used for picture compilation and basic C2 for specific warfare functions i.e. anti-air warfare. Those systems are generally slow, at least by modern data communication standards. Their most important limitation however, is their inability to cooperate with each other and immediately share data as they have been developed to satisfy segregated needs. Teletype circuits are not data friendly as they are incapable of transmitting data in any other form than text with Baudot coding at 75 baud usually. Moreover, information exchange between a teletype circuit and tactical systems is impossible without a "gateway," usually human. Voice circuits are indispensable for some functions, yet information passed over a voice channel is limited. Link 11 and the future (NATO-wide) Link 16 use incompatible message formats (Henderson, 1996).

In the current architecture, there exist procedural/organizational shortcomings as well. It is interesting to note that the USN has also faced the same shortcomings some years ago when it initiated the Copernicus architecture. (Turner, 1992) Those have been:

- The sub-optimal systems development. Since systems have been developed on a case by case basis, even the best efforts in ensuring optimality for every system does not guarantee optimality for the "system of systems."

- Traffic separation. Administrative and operational traffic usually share the same media, resulting in cumbersome methods (minimize, screening) for traffic minimization during periods of heightened operational tempo.
- Message format. The narrative, paper kingdom is prevalent. Formats such as audio or imagery are not possible to use with the existing infrastructure. Moreover, correlation of data becomes more difficult as the human decision-maker is required to perform the task without automata helping him.
- Traffic overload. The multitude of systems operating in one area and the variety in data formats describing the same environment result in loss of resources due to duplicity of effort. The ideal would be, for every target to be in one location report over the entire system at any time.
- Lack of unity of purpose. The various systems do not have a synergistic effect in supporting the mission, and many times are in conflict with one another. Classic example is the EMI problems on the *de facto* limited space of a ship.

Furthermore, at the architectural level there is not a formal process to help define an appropriate architecture. To avoid those shortcomings the HN has to define a suitable information architecture and utilize it for the development, deployment and operation of its information systems.

2. Components of a desired information architecture

For an information architecture to be successful, it must contain the operational, technical and systems requirements for the deployed information systems. (C4ISR ITF, 1996) The operational architecture should describe information flows that support the

end node (usually ship or command at sea). The format of information, the frequency of information exchange and the supported tasks are included in the operational architecture. The technical architecture focuses on technical standards, interfaces and the engineering specifications of the architecture. The systems architecture incorporates the physical layout of systems, and defines the boundaries for measures of merit. "The systems architecture is constructed to satisfy operational architecture requirements per standards defined in the technical architecture." (C4ISR ITF, 1996)

Components for an information architecture are shown in Figure 5.

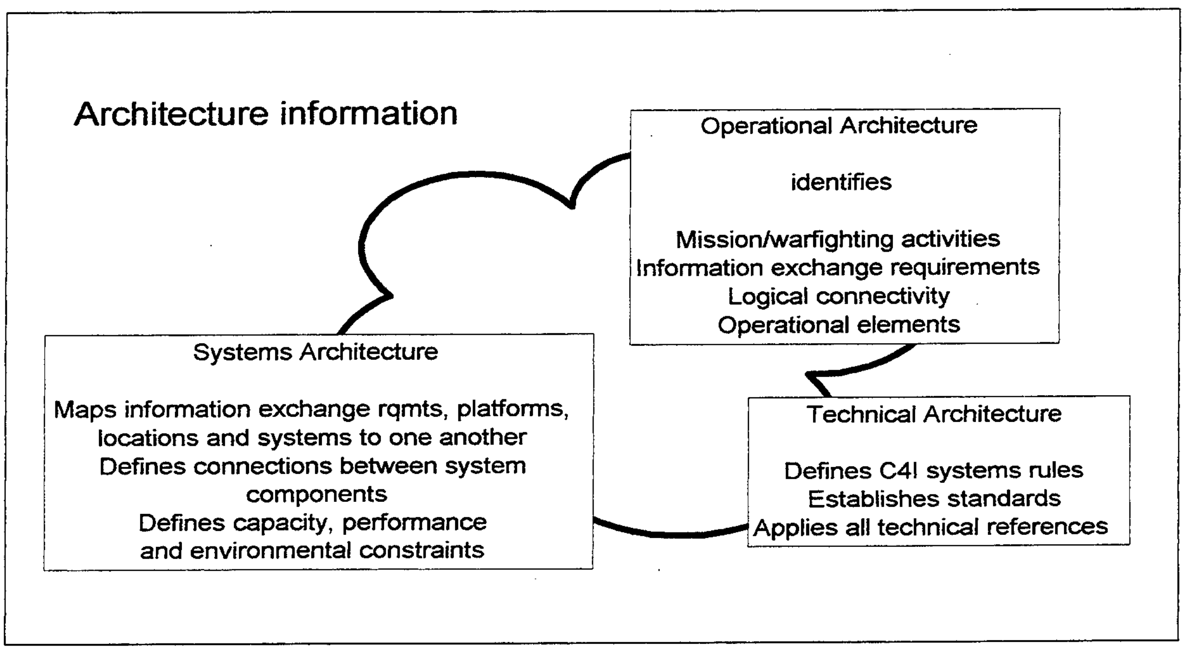


Figure 5. Components of an architecture (After C4ISR ITF, 1996)

C. SCOPE

This thesis attempts to identify the steps needed in a definition of requirements for a new HN information architecture, through a presentation of two real life model projects. In Chapter II, a review of suggested methodologies used to develop information architectures is employed to establish a set of suggestions for a future similar HN venture. In Chapter III, the "SeaNet project" adapted from the synonymous project at the Naval Postgraduate School, is used to support the ideas underlying an infrastructure-application architecture. Finally, the thesis examines in Chapter IV potential benefits of launching a small-scale pilot project, such as the "HF e-mail" project by MITRE as part of the transition to the new architecture.

II. DEVELOPMENT OF AN INFORMATION ARCHITECTURE

A. GENERAL

1. Review of information architecture concepts

The IEEE definition of an architecture is: "The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time." (IEEE STD 610.12) However, in discussing information architectures the IEEE definition constraints us to think only in terms of information areas (components) that are disjoint from the functions they serve. (Khosrowpour, 1994) If an organization is seen as an information processing system, the mission of the organization must be reflected in the way information systems are set up. A more inclusive definition for an information architecture then should incorporate the supported functions along with the information systems and their interrelations. Grenier and Metes propose such a definition: "An architecture is a system of constraints and definitions that forms a framework *for providing products and services*." (Grenier and Metes, 1992) For the HN, the promulgation of an information architecture constitutes a major challenge since the products (missions) have expanded at the same time the systems available to support them are becoming obsolete.

Information architectures contain several models of sub-architectures. Taking their input from two fields, business needs and information technology, information architectures are usually analyzed in an application architectural model (or systems architecture), a technical model, and an organizational model. (Scheider, 1996) Some

authors identify one more category, the data model (Scheider), while others consider it as a substrate for all architectures (C4ISR, Spewak) The layout of different architectural models as well as a generic time direction of the process for their promulgation is shown in the following figure.

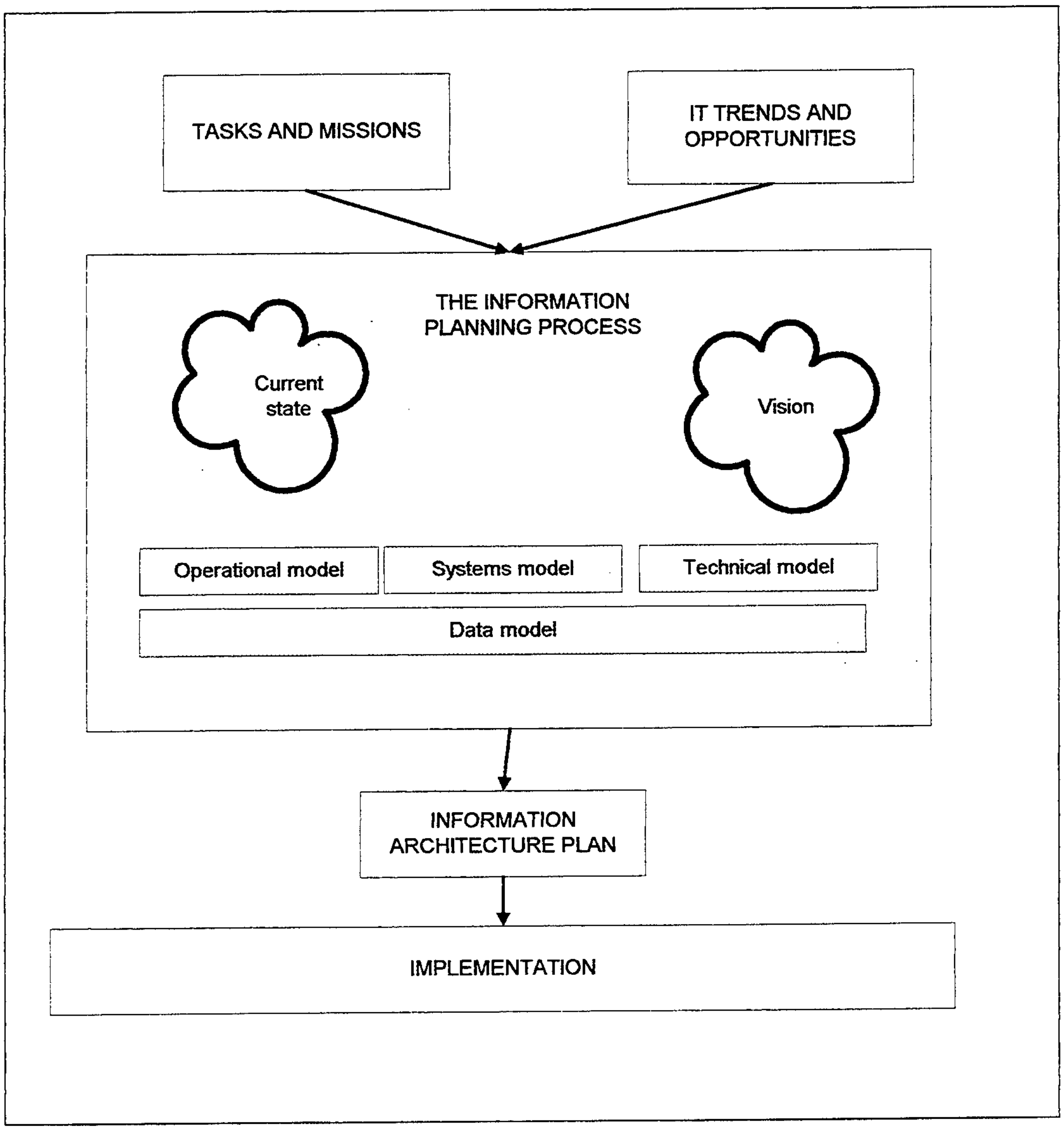


Figure 6. Generic structure of an Information Architecture Planning Method (After Spewak and Hill, 1993)

The first two blocks of the figure constitute the awareness phase in developing an information architecture. The organization examines support given to its tasks by current information systems and compares it with potential support, offered by new information technologies. The information planning process is then depicted below as a separate box because the elements described in that box should not be in a particular hierarchy as they are continuously re-assessed. For the Hellenic Navy in particular, the information architecture planning process should not assume an architecture in place. The extent of stovepipe systems deployed and the lack of standardization in existing information services, make it more rational to focus on the future vision, with the existing situation defining the resources and commitment needed to achieve the "ideal" architecture.

The models shown within the planning process are --usually-- graphical depictions of the architectural components. Different methodologies use different tools to communicate these components to the interested parties. Functional decomposition diagrams, entity-relationship (E-R) diagrams, matrices, data dictionaries or even abstract mind-mapping schemas can be employed. Nonetheless, any operational model should describe the tasks, operational elements, and information flows required to accomplish or support a given function. The systems model should describe the interconnections of systems supporting the functions. Technical models should describe the infrastructure and how systems can get services from it. Systems and technical models have a direct relationship with the physical world, representing topologies and their interactions (lower layers), whereas the operational model follows the upper layers of an architecture. The implementation part of the process includes feedback mechanisms to facilitate the enforcement and revision of the architecture.

The objectives of an information architecture have been better *manageability*, *integration* and *stability* for the information systems of an organization. An information architecture is an effective tool in the management of information systems by providing: (Khosrowpour, 1994)

- A basis for re-designing business and IT structures. Information architectures are meant as forward looking analytical tools for achieving optimization. To successfully develop an information architecture, a vision of an ideal state for the information systems and their exploitation by the organization is required.
- A blueprint for the development of future information systems. The transition from the current state to the envisioned needs to be specified within the architecture. Organizational learning is also dependent on the ability of the framework for developing an information architecture to analyze *a posteriori* decisions and review procedures and practices. The architectural framework could also serve as a knowledge repository for strategic planning.
- An effective means to prioritize and control IT procurement. Information architecture provides the unity of purpose for the procurement and product selection processes. As an example, a program manager responsible for procuring a radar might consider the capability of the radar to connect to a network hub or have installed management agents as an extra expense. If the information architecture identifies the same radar as part of the network-centered system, then the necessary interface becomes a sine qua non.

Integration of information systems is important in achieving a synergistic effect towards the support of the business functions. That integration of separate information

systems however can be of different types. (C4ISR, 1996). One is integration between hierarchical levels. A future Navy information architecture employed by Hellenic Fleet commands for surveillance could be related to a joint maritime architecture, serving national needs. Different architectures at the same hierarchical level could be integrated as well. For example, an operational architecture for naval anti-air warfare could be coordinated with the air defense ground environment for resource sharing. Stability is served by information architectures because it separates the short term tactical considerations in IT planning, such as the decision to acquire a particular system or not, with the long term strategic considerations about any system's interface with the information infrastructure.

The process for defining an information architecture follows a pattern of cycles. Attempts to identify available technologies for supporting business functions, experimentation with and adaptation to the technologies, their subsequent rationalization and establishment within the boundaries of the organization and finally their widespread use, comprise those cycles. (Burn and Caldwell, 1990) If we return to the generic structure of an information architecture planning method, we recognize that changes in the environment of the information architecture (i.e. tasks and missions, IT, feedback from implementation) create tensions to our planning process. The methodology adopted for the definition of the information architecture is at least as important as the architecture itself, since it is required to continuously be able to adapt information architectures to different environments. The following section examines traditional methodologies used for defining information architectures.

2. Methodologies used for developing information architectures

The question that this chapter addresses relates to the development of an appropriate information architecture. However, the focus is not on the architecture itself. Instead, we concentrate on the methodology required to address successfully the task of promulgating an appropriate information architecture. Several different types of methodologies exist for developing information architectures. Spewak and Hill differentiate methodologies in process-driven versus data-driven or technology-driven versus business-driven. Based on the Zachman framework for architecture development they propose business and data-driven methodologies. Davis and Olson suggest a typology of five different classes of approaches for the determination of information requirements at the organizational level. These are: (Khosrowpour, 1994)

- Normative analysis. It recognizes that information needs can be thought of in advance, and information systems can be then designed based on those needs. After their deployment across the organization, differentiated needs can be met with ad hoc adaptations. This approach could serve well stable organizational environments with little diversity in information needs among the members of the organization. It is basically, a bottom-up approach. A military organization, can not rely solely on such an approach to fulfill and coordinate its varying information needs.
- Strategy set transformation. A top-down approach which focuses on business goals and their support by information systems. It is useful for prioritizing systems according to their utility for the organization.
- Critical factor analysis. Also a top-down approach which has as its starting point the critical success factor for completing tasks within the organization. Its utility is also

in prioritizing information systems. Both of the two last approaches assume that top management has a clear vision of what the information needs are and are not particularly concerned with input from the lower levels.

- Process analysis. Organizational processes are grouped in functional areas under this approach. It results in functional decomposition diagrams which describe the business functions in hierarchical terms. Methods falling within this approach are usually well defined and there is an extensive literature to support them, however they assume functional areas as independent of the organization structure.
- Ends-means analysis. A systems analysis approach that defines information requirements in terms of inputs and outputs of different subsystems. Methods using such an approach are particularly suited to define boundaries and are particularly useful in projecting opportunities available to the organization by changes in information technology.

One factor contributing to the existence of various approaches is the variance of purposes an architecture serves. The Integration Task Force of the US Department of Defense identifies the following purposes served by an information architecture, in a military organizational environment: (C4ISR, 1996)

- Developing joint requirements for program mission need statements and operational requirement documents.
- Identifying and prioritizing C4ISR system deficiencies and allocations in context with joint needs.
- Improving interoperability and identifying opportunities for integration.

- Determining policy/doctrine, system support needs, and application/infrastructure support needs for specific joint warfighting functions.
- Identifying communications connectivity and capacity requirements.
- Measuring systems strengths and weaknesses with respect to supporting joint operations.

A multiple methodology approach is needed to include all aspects an information architecture covers. Earl concludes that using only one methodology will not work (Khosrowpour, 1994) He suggests that multiple methodologies are more appropriate for changing organizations. Multiple methodologies include a top-down approach integrating business goals into the information architecture, bottom-up components to account for the existing information systems and an inside-out component which describes the planning help provided by think-tanks, and software tools such as expert systems for strategic planning. The last component translates opportunities present in the environment to terms "usable" by the other two. The challenge to define an appropriate architecture becomes one of coordinating the above methodologies instead of selecting only one of them. Two real life approaches, one from the business world and one from the defense community are reviewed in the following Section. The business model has been selected because it is considered as visionary and integrates many elements of the network-centric vision for information systems mentioned in the introduction of the present thesis. The DOD paradigm is useful for it directly relates to the type of tasks and missions the Hellenic Navy is expected to undertake. The final Section of the Chapter suggests a set of propositions for further research in an attempt to initialize a discussion for the development of an information architecture appropriate for the Hellenic Navy.

B. MODELS OF INFORMATION ARCHITECTURES

1. Capability based model

Grenier and Metes, expanding on a project that "brought together" information systems from McDonnell Douglas, Northrop and the USAF during the development of the prototype aircraft YF-23, define an organizing principle for information-dependent organizations, the Capability-Based-Environment (CBE). It is defined as "a multi-organizational, cross-functional community that uses electronic information to design, sustain and manage work and to evolve its own capabilities to learn and to perform over time." (Grenier and Metes, 1992) The environment then becomes a system of "commitments, capabilities, technological artifacts, work processes and strategies.[2]" The model itself is generally --abstraction is intended-- comprised of three interdependent aspects: The work environment, the capability-based environment and what the authors term simultaneous distributed work. Here, we are not focusing on the abstract aspects. Rather, we intend to show the utility of specific parts of the model for our planning needs in designing an information architecture.

One important concept of the model is the *use of networks*. Networks are considered as parts of a given information technology as well as a means of communication in the broad sociological sense. Networks are the center of the universe, and are considered enabling structures which incorporate high performance, openness, connectivity, flexibility, interoperability and manageability. An adaptation of their networking concept is depicted below, for a military environment.

[2] All quotations in this subsection are from (Grenier and Metes, 1992) unless otherwise noted.

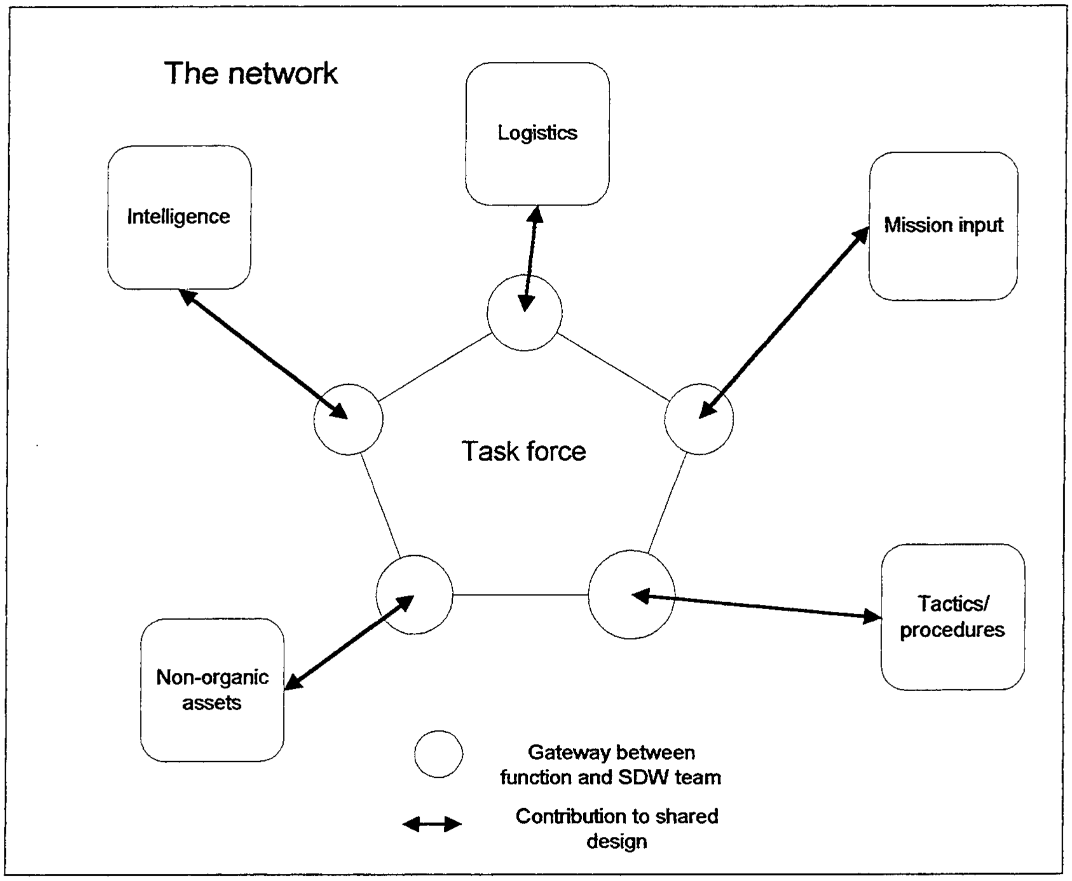


Figure 7. A network centric view adapted from the CBE model for a maritime task force

"Networks enable the quick and easy movement of information in al electronic forms to all stakeholders." The added value by networks in the organization is due to the following factors:

- They provide access to distributed information and knowledge.
- They allow electronic communication among persons.
- They are proactively built to meet future needs.
- They extend the reach of the organization. Here organization is describing a group connected by a "unity in purpose."

Networks are comprised of logical rather than physical nodes, and --again-- logical communications links. In the CBE networking construct "unity of purpose" becomes the metric for defining utility, and leadership replaces administration or control. The concept of network management as a set of concentric circles extending from the physical nodes to the enterprise is similar. The relationships that connect distributed work to networks are reflected in the following architectural attributes:

- Connectivity. It is designed to provide flexibility through open communication standards.
- Interoperability. The methods for ensuring interoperability range from the selection of the gateway to the application development.
- Manageability. Manageability is a combination of systems that address fault analysis and resolution, configuration management, performance management, security management, accounting management, and applications management.
- Performance. Performance provides the measures that enable us to determine the value added by the network.

One cannot escape the direct similarities with command and control functions and the nature of military operations. It becomes more apparent when we review the authors' view of the leadership's responsibilities:

- Clarity
- Articulation of purpose
- Support, motivation and reward
- Issue resolution
- Effectiveness of communication and

- Creation and maintenance of commitment to the CBE model and SDW processes

The assumptions the CBE model makes are similar to the challenges recognized in the introduction of the present thesis. Organizational and technological change, the need for distribution of work to the units most fit to perform it, the recognition that knowledge is the critical resource, and the realization of time constraints are well established realities in the navy's working environment. The benefits from investing in a capability based model are realized from the preposition of capabilities, so that time between event and adaptation is minimized. This concept has long been a requirement for military communications.

The actual design of the information architecture is based on the needs of the "working community." Design parameters include the connectivity needs of distributed work teams, the types of information to be transferred, the appropriateness of technologies to the business ethic and the availability and interoperability of information applications. Working groups (in the navy's paradigm collaborating forces) are differentiated in two dimensions: spatial and temporal dispersion. The following figure shows a matrix describing those relations.

The overall design of the architecture should be tested --according to Grenier and Metes-- for capability, testability, manufacturing (reliability) and disassembly (scalability). In the final chapter of their book, they include a benchmarking method for classifying an organization within the capability based environment.

	Synchronous	Asynchronous
Distributed	Mission update	Broadcast services, intelligence updates
Co-located	Task organization, warfare functions allocation	Training

Figure 8. Matrix for types of exchanges between groups in CBE

2. C4ISR (DOD)

The C4ISR Architecture Framework was developed under the auspices of the C4ISR Integration Task Force (ITF) Integrated Architecture Panel (version 1 promulgated in 1996.) Its objective is to "define a common approach [for defense agencies] ....in developing their information architectures."

> "Once adopted, the Framework will provide a common basis for developing architectures that can be universally understood and readily compared and contrasted to the other architectures, It will facilitate the reuse of architectural information and results and will serve as the foundation for expansion and integration of architectures across organizational and functional boundaries. In addition,....will promote effective communications between warfighters and system developers....Ultimate potentials include....improving compatibility, interoperability, and integration among C4ISR capabilities." (C4ISR, 1996)

Here, we focus on the component models of an information architecture --as it pertains to a military organization-- and on the products deliverable for each model. Interrelationships among the models are shown in the following figure:

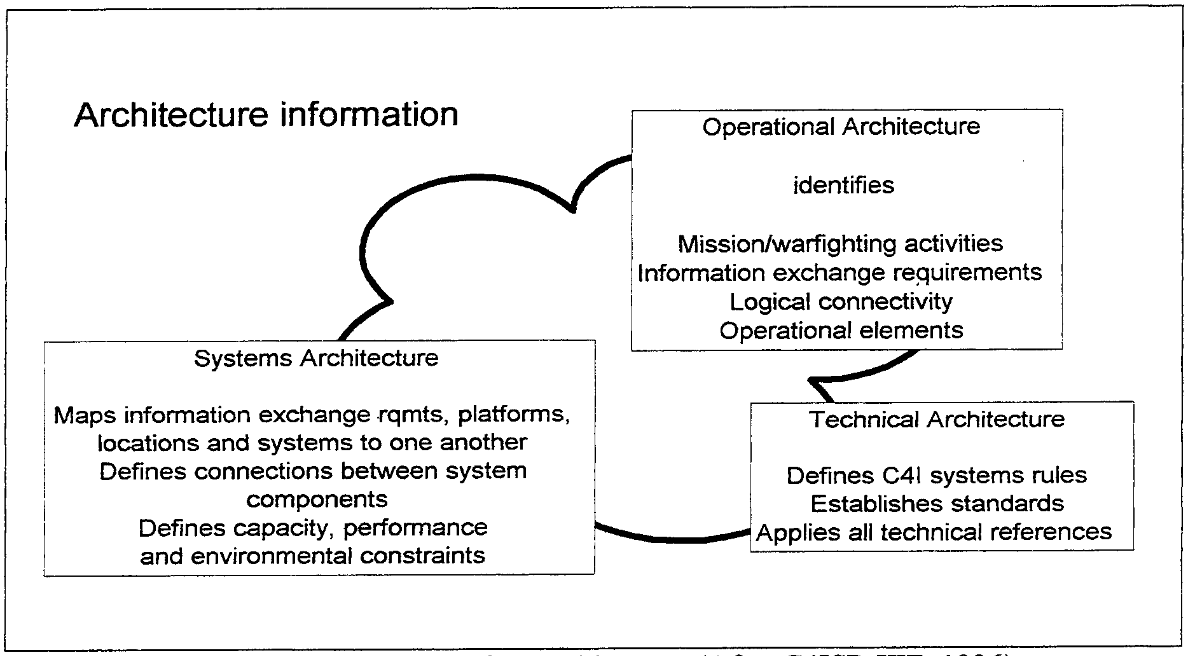


Figure 9. Components of an architecture (After C4ISR ITF, 1996)

The guiding principles for the development of the framework are similar to those adopted by the CBE paradigm. Facilitation of user understanding and communication among users, the establishment of a benchmark for comparisons and integration, and the need for a modular, expandable and reusable architecture complement the overarching need for establishing a clear purpose for the architecture. The systems to be integrated in a command and control information system include a variety of sensors, decision nodes, communications channels and action nodes. A clear identification of the purpose will

provide the background knowledge necessary to integrate them in a coherent and effective supersystem.

The specific models of the system have different characteristics and different tools are used for their presentation. The C4ISR architectural design focuses primarily on the operational architecture. The operational architecture itself uses a top-down functional decomposition to define tasks, operational elements and information flows. An important departure from traditional architecture design is that operational architectures should not be designed to fit particular force structures. Therefore, they become dependent on the mission itself and not on the organization employed to serve the mission. Current developments in NATO structures, with the evolution of ad hoc Combined Joint Task Forces are conformant with such architectural concepts. Deliverables for an operational architecture are structured around information exchange requirements (IER). "They identify *who* exchanges *what* information with *whom*, as well as *why* the information is necessary and *how* that information will be used." (C4ISR, 1996) or "an inventory of sensors, decision support and actors." (Buddenberg, 1993)

Systems architecture is driven by the operational, since it maps information systems to operational elements. It defines boundaries for systems and their interfaces, and it is technology- dependent. Nonetheless systems architecture should not be constrained by the status of deployed information technology since architectures provide vision. It is the connecting link between technology and mission needs. Critical information for defining a systems architecture is the operational tasking of nodes as senders, processors and/or receivers of information. Nodes could be a task force or a single workstation depending on the level of the architecture.

Technical architecture defines the set of rules that govern systems implementation and operation. They are based on a comparison between requirements stated by the systems architecture and possible enabling technologies. Focus is on open standards and the need to incorporate multi-platform networking interconnections. Essential information for a technical architecture is the set of services, standards and configurations to be implemented.

The development process for the architecture follows a series of steps, resembling the generic process we defined in Section A. Architecture developers for a C4ISR architecture should: (C4ISR, 1996)

- Determine the intended use of the architecture.
- Determine the architecture's scope and context to include assumptions or constraints.
- Determine specific architectural characteristics.
- Determine the architectural products to be build and
- Build the architecture.

A sample use of architectural products is shown in the next table.

C. INFORMATION ARCHITECTURE FOR THE HELLENIC NAVY

From the discussion above and the two examples for the development of information architectures a set of propositions can be made for the benefit of a future Hellenic Navy similar effort. However, before defining specific architectures a framework for their development should be promulgated. Benefits from the framework approach relate to organizational learning. It also provides a common basis for

Sample Questions	Operational	Systems	Technical
Who needs the information ?	Operational concept diagrams Command relationships charts		
Who produces the information ?	Operational concept diagrams Command relationships charts	Supporting Systems Diagrams and Descriptions	
Do the means exist to convey the information from the producers to the users?	Operational concept diagrams Node connectivity diagrams	Systems Data Flow diagrams	Information Standards Descriptions
Do systems have the set of enabling functions necessary to conduct the required information transactions?	Activity Diagrams Data models	System Overlays Activity Allocation to System Component Descriptions	
Are the enabling functions implemented in accordance with standards?		Supporting Systems Diagrams/Descriptions	Information Standards Descriptions

Figure 10. Sample Use of Architecture products (From C4ISR ITF, 1996)

comparisons between architectures and allows us to achieve better understanding of what an architecture is. The assumptions and constraints can also be incorporated in the framework, making easier the update and review of the architecture. Specifically for the case of the Hellenic Navy, since there is not any other architectural model in place --at least known to the author-- such a framework could be used for developing integrated architectures across the three Hellenic Armed Forces services.

The architectural framework must be based on the following tenets to ensure the three main objectives of an architecture, namely *manageability*, *integration* and *stability*:

- The overall theme to be served by an architecture is to ensure unity of purpose for information systems in supporting the organization's missions. C^2 in particular has unity of purpose as its organizing principle.

- The technical artifact to implement unity of purpose through an architecture is the concept of the network. Metrics for network utility within an architecture should be based on their availability and survivability primarily and secondarily on security (capacity next).
- Networks consist of links employed to serve nodes. Nodes must be able to seamlessly communicate information with other nodes using data in various formats. Nodes include systems and humans that use them. Services to be supported are shown in the next table:
- An architectural framework should differentiate between the operational, technical and system architectures.
- Management of the network is not confined to administration but includes functions to support the role of leadership.

Services to be supported by networks
Process-to-process message passing
Distributed file and database manipulation
Teleconferencing
Video monitoring of environment
Time synchronization
Name or directory services
Voice distribution
Network and system management
Security services
Image services
Email (within node, between nodes and across the infrastructure) and messaging

Table 2. Services to be supported by data networks (After Bradner and Mankin, 1996)

- The network should not preempt the organizational structure. For example the same network should support centralized and decentralized decision making organizations as shown in the next figure:

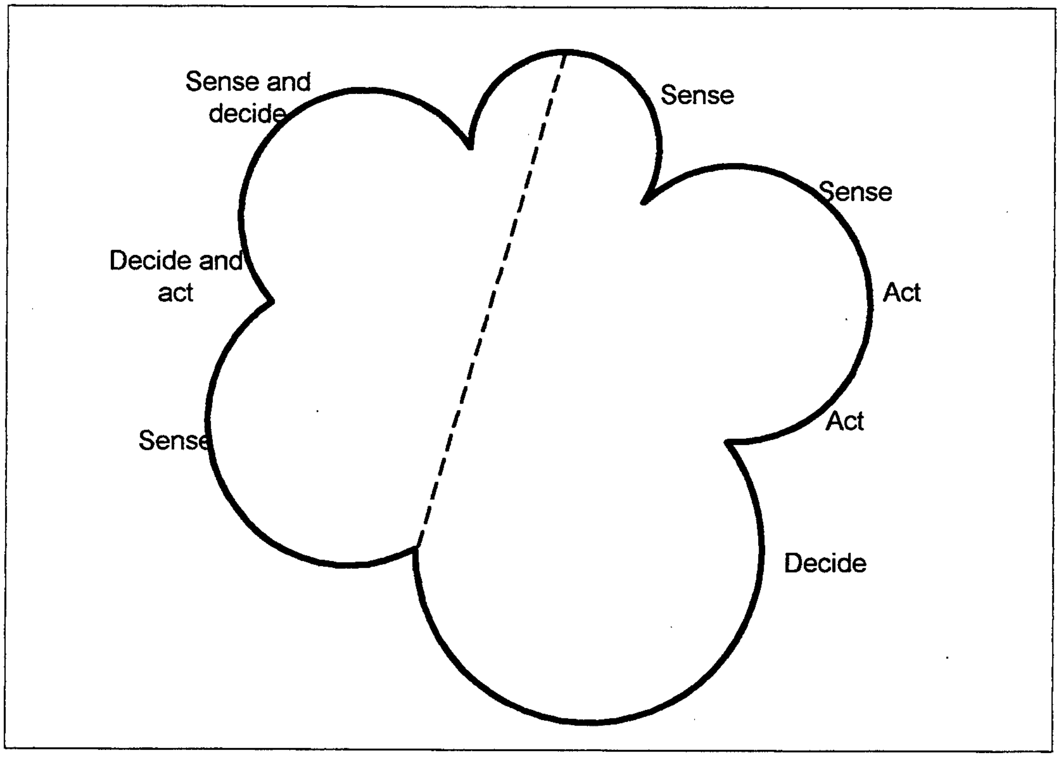


Figure 11. Centralized and decentralized decision making supported by a common network

- The technical architecture should provide the standards profile for interconnecting with the network. A recommended standards profile by Buddenberg is depicted in the next figure. It is considered a low-risk, generic profile where any omissions represent growth options. Furthermore, it sets a framework for categorizing standards.

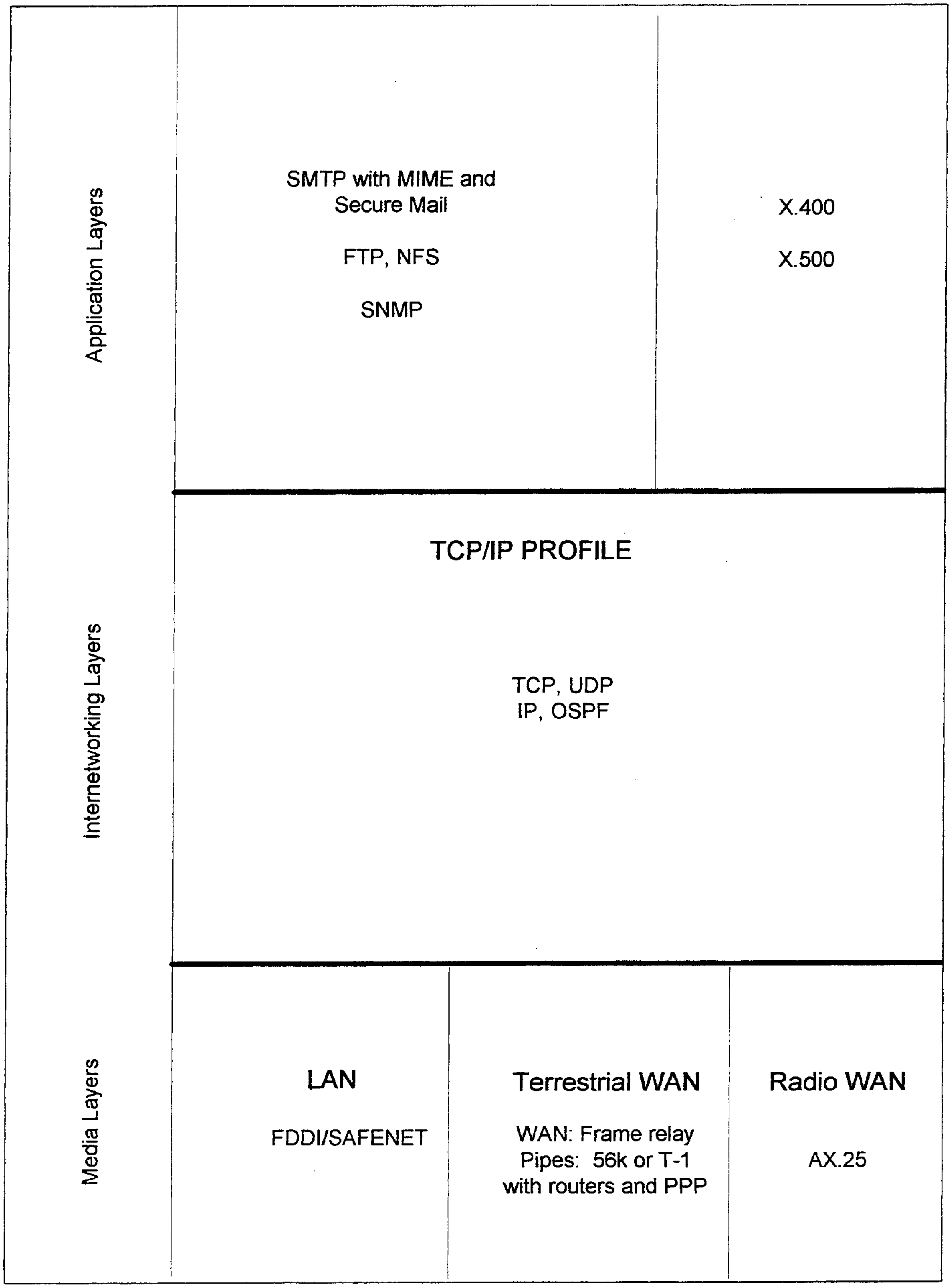


Figure 12. Recommended Standards profile

The challenge for the Hellenic Navy is one of successfully absorbing information technologies. Effective absorption requires that managers understand and provide capabilities for five major functions: (Khoseowpour, 1994)

- Technology forecasting and evaluation
- Pro-active information requirements definition
- Pro-active business process re-engineering
- Business process integration and
- Appropriate project selection and implementation.

Two projects will be reviewed in the following Chapters to exemplify the concepts discussed above.

III. INTERNET AT SEA

A. BACKGROUND

Extension of data communications to Hellenic Navy vessels has not gone beyond the technologies that stovepipe tactical data links, slow teletype traffic over HF links, or expensive and stand-alone INMARSAT connections offer. The requirements of speed and interaction among sensory, decision or action nodes in a C2 environment are not met by deployed technologies. A number of developments facilitates the extension of Internet based data services to seagoing platforms: (Buddenberg et al., 1996)

- Community awareness. Using the Internet at the office ashore or at home, people are questioning why they could not exploit the same functionality in the seagoing environment.
- Carrier infrastructure developments. Expected low cost worldwide communication services offered by the operation of low earth orbiting satellites (LEO) as well as data communication services offered by the Hellenic Telecommunications Organization (OTE), or by commercial GSM-cellular companies (Panafon, Telestet) allow information exchange via means other than HF radio for units afloat.
- Protocol maturity and industry convergence. Even though --particularly at the data link layer-- terrestrial Internet protocols do not map well to radio/satellite WAN characteristics, protocols allowing medium access for many users are being developed. Also, there is an expected convergence between the satellite industry and the Internet due to the growing commercial potential of the latter.

The present chapter is based on research conducted under the "SeaNet Project" since 1990, whose main purpose is to provide transparent Internet connectivity for ships in the oceanographic research fleet *routinely*. (Buddenberg et al., 1996) Although focused on the needs of the oceanographic community, adaptation of the project's elements to fit naval or coast guard needs is minimal, if any. Key research objectives of the project that appear relevant to the needs of Hellenic Navy and a brief discussion is deemed necessary as an introduction to the present Chapter. Those SeaNet research objectives are: (Buddenberg et al., 1996)

- To provide communications systems to ships that enable them to transparently access the shore-based Internet. Extension of the Internet to shipboard communication nodes affects four distinct areas for development by the Hellenic Navy. (1) The shipboard communication node must be able to take advantage of the technologies IP connectivity offers. (2) The shore based infrastructure must be able to support the requests for service by the mobile components, support remote management of the network components and allow for dynamic topologies of the networks.(3) Command and control (C2) tasks have to be re-engineered, taking advantage of the new technological capabilities. And finally, (4) HN must develop the knowledge to plan, develop, operate and manage a similar project on its own, while integrating wider national needs (disaster relief ops, support of the national information infrastructure, provide a test-bed for research) to the venture.
- Provide initial subsidies for communications costs in order to minimize the initial development costs associated with the project. The Coast Guard and academic institutions can support the Hellenic Navy's effort. European Union funding could

also be a possibility since the project might be incorporated in research aiming to extend personal communications services (PCS) services to mobile users in areas with minimal telecommunications infrastructure (Re, 1996) Another source of funding and support might be provided by the Greek shipping industry since it would extend obvious benefits for its operations. (i.e. communications at a lower cost, Tele-medicine, Tele-maintenance and conferencing) A draft estimated budget for the actual SeaNet project is shown as Appendix A, along with some explanatory notes to provide a guide for the costs associated with a similar project.

This thesis uses the SeaNet project-based modular approach to suggest a networking paradigm for the Hellenic Navy based on the concepts discussed in Chapter II for a network-centric information architecture.

B. MODULES

1. Shipboard LAN

The shipboard LAN can be developed independently from the rest of the project. Value can be gained from installing shipboard LANs since they would provide computer resource sharing, sensor interconnection, and office automation intra ship. A visionary LAN would look like figure . The visionary shipboard LAN should have a backbone LAN running across the ship with several stubs that allow interconnection with other LANs or individual sensors. The recommendation in the SeaNet project is that the backbone LAN should be patterned after the US Navy's SAFENET standard.

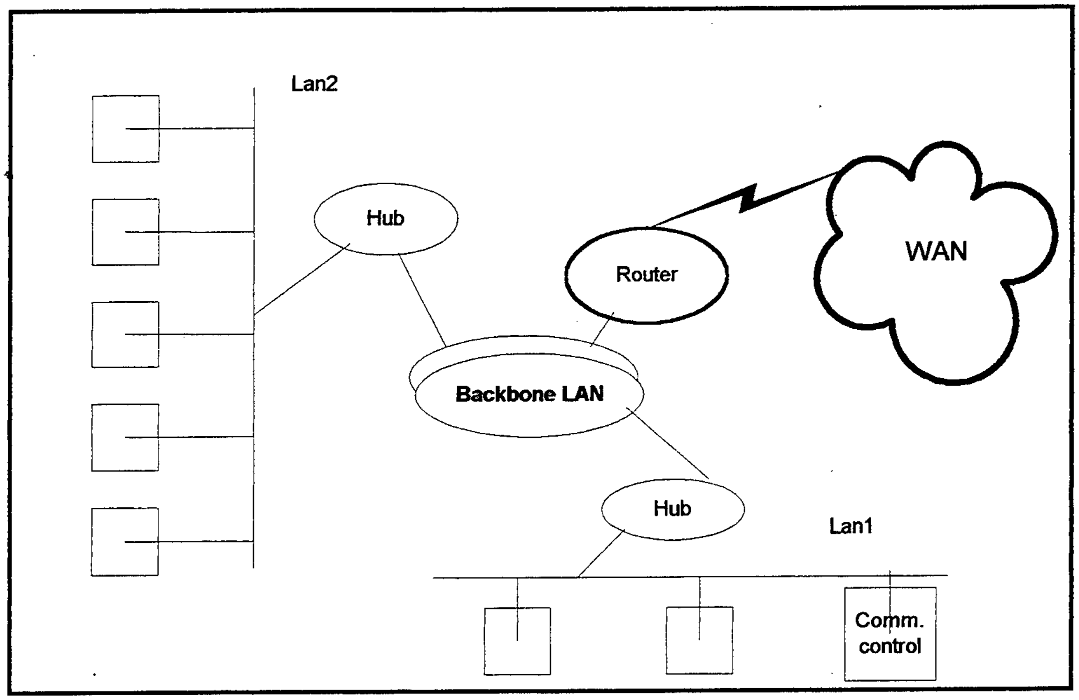


Figure 13. Shipboard LAN vision (From Buddenberg, 1993)

SAFENET uses Fiber Data Distributed Interface (FDDI or X3.139) and provides the following benefits: (Kim and Muehldorf, 1995)

- High reliability and survivability for shipboard communications. It uses two counter-rotating fiber rings.
- Rapid and frequent automated fault detection, isolation, and recovery, by exploiting the ring wrap capability that the two rings provide.
- It has a bandwidth allowing data rates of 100 Mbps, minimizing transfer delays of critical data. Research though promises higher rates on the same cable. (Buddenberg, 1993)
- It uses OSI compliant standards and allows for the GPS timing protocol.
- Fiber cables do not emit electromagnetic interference nor are they affected by it.

The LAN segments (LAN1,2 in Figure) represent divisional or departmental LANs within the ship. Ethernet (10Base-T) is well suited for their use. LAN segments are connected to the backbone through hubs, that must be pre-positioned as outlets in places where sensors or networks are expected to be since connecting to optical cable requires more effort than connecting UTP cable (used for Ethernet). Sensors attached to LANs should be able to disseminate their data with strict requirements for speed and reliability. Management of sensors as well as network devices is discussed below. Hubs should provide connections for both the FDDI ring and the Ethernet(s). Critical networks or sensors should be connected to the backbone with Uninterrupted Power Supply (UPS) hubs.

Internetworking capabilities are provided through the ship and with the outside world via the router. It is the "connecting medium" of the SeaNet project and is required to interconnect shipboard LANs to the radio WAN services. It must be able to handle any network layer protocols used. For routing protocols Tanenbaum suggests different routing protocols for within the local network (he terms it an Autonomous System) and for routing outside the AS since different optimal characteristics in internal and external routing are required. OSPF should be used within the AS (interior gateway protocol) -- as it is more transparent -- and BGP (current version is BGP4) as the external (exterior gateway protocol). The AS level represents a number of routers reflecting a Navy battle group. BGP masks the network internals to the outside viewer. BGP also supports policy routing and policies are manually configured to the router. (Tanenbaum, 1996) An example of policy routing is: "Do not transit traffic from Albania."

The router should be a managed device conforming to the Simple Network Management Protocol Version 2 (SNMPv2) The ability for remote router management could thus be available to shore command stations over the WAN link. The issue becomes one of command and control semantics and not one of technical feasibility. Capacity of the router should not be of primary interest since the capacity of the system has as a bottleneck point at the WAN link. However, the router should be powered by an UPS.

Network management capabilities should be installed as part of the ship package. Network management should address all of the following categories: (Grenier and Metes, 1992)

- Network fault analysis and resolution management
- Configuration management
- Performance management
- Security management
- Accounting management
- Applications management

The SNMP protocol allows for the Remote Monitoring (RMON) protocol that has as standard features remote probing (passive derivation of management information) as well as remote monitoring (manager to manager interaction). The following figure depicts the RMON management scheme. (MIB is the database of management objects.)

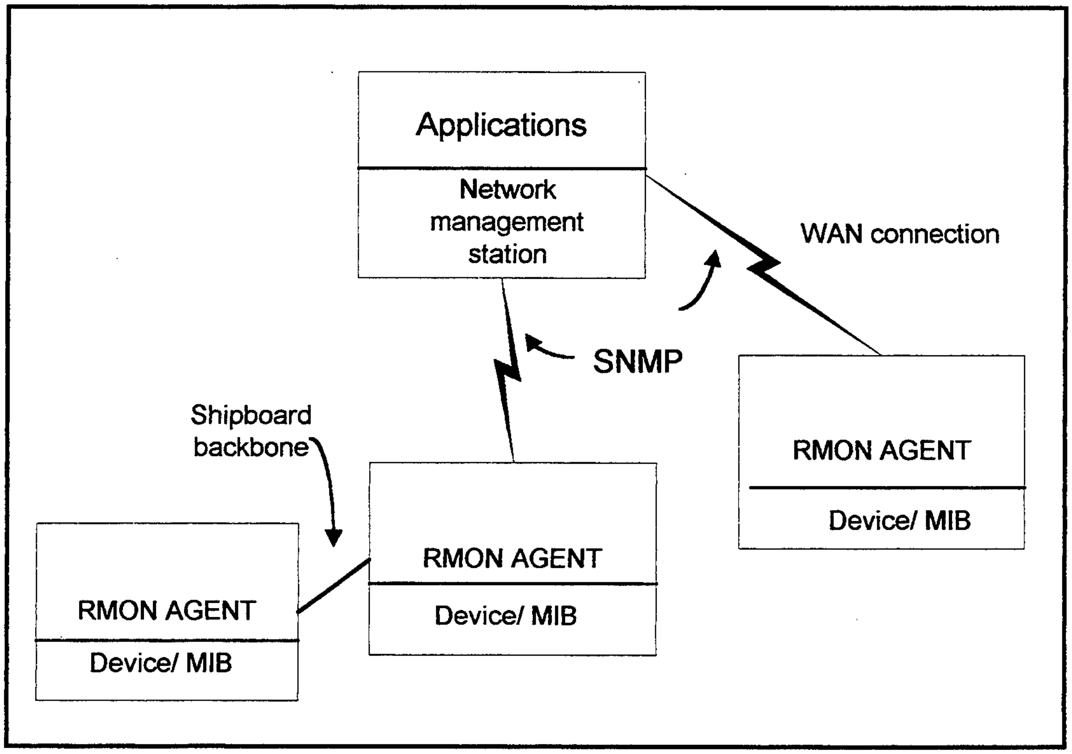


Figure 14. Remote management using SNMPv2

2. Connectivity with terrestrial infrastructure

The land-based infrastructure provides extended geographical reach for the networks at sea through the radio based WAN. The requirements for a WAN service to be used by the project is high availability, interoperability with our protocols and capacity. Cost becomes a factor in deciding the nature of services to be requested by the land-based infrastructure provider. (Buddenberg, 1993) Other factors to be considered include coverage area, reaction time and connectivity with Internet Service Providers (ISP). A generalized model of the network would look like the figure below:

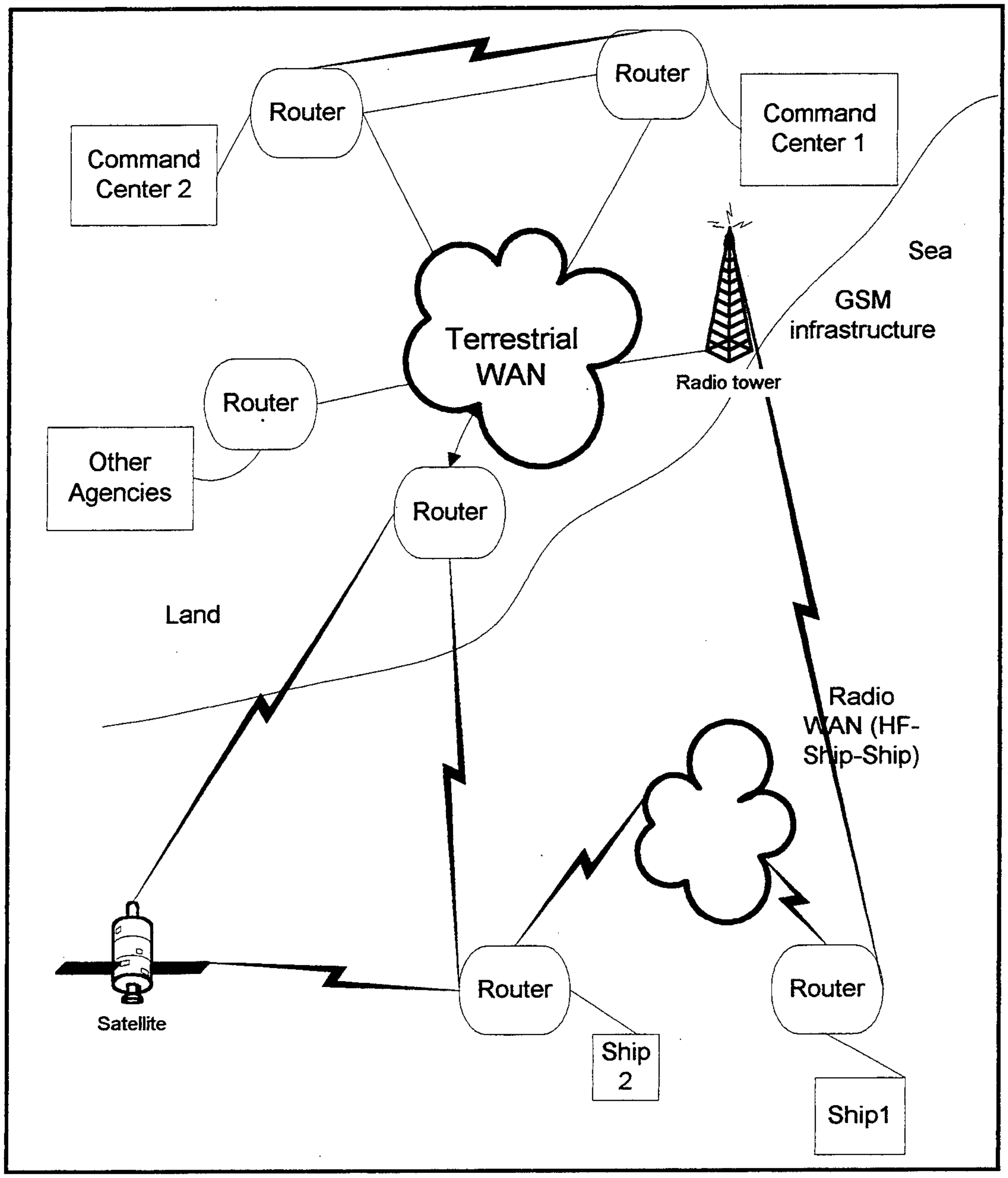


Figure 15. A model network of networks based on the SeaNet project

The requirements for efficient operation of a SeaNet-like network of networks for the Hellenic Navy dictate the need for alternate routing provision between ships and

commands afloat and the networks and services located ashore. Radio connectivity could be provided by one or more of the following means:

- HF-VHF radio. A cost-free medium for exploitation. Problems associated with data communication using the HF medium are analyzed in Chapter IV. Here we note the limited capacity and high error rates. Real-life projects have achieved 4800 bps speeds and are expecting 9600 bps connections with advanced modulation techniques.
- GSM cellular. Its coverage is limited geographically, however in the Aegean environment with the commercial interest for the extension of cellular services to the islands a growth in coverage is expected. Appendix B is a coverage map provided over the Internet by one of the cellular companies in Greece. Alanko and others at the University of Helsinki have experimented with transmission of TCP/IP packets over GSM connections and have provided link establishment times for dial-up connections not exceeding 35 seconds, and effective transfer rates of 240-800 Kilobytes per 15 minutes (2184.5-7281.7 bps), depending on transmission conditions. Error rates were of the $1*10^{-8}$ magnitude. (Alanko et al., 1994)
- INMARSAT-B (HSD) service provides 64 kbits/sec service comparable to basic ISDN wireline services.
- European research towards an integrated environment for future mobile communications includes satellite communications as one of its components. The COST 227 and COST 252 projects intend to provide the framework for seamless integration of the cellular infrastructure with satellite supported communications. (Re, 1996) LEO satellite solutions can also be considered making the decision

problem one of economic analysis instead of technical since there seems to be a convergence of provided services. Here however it should be noted that from the three LEO consortia, only the little LEOs are oriented to support packet networks. Big-LEOs support seamless integration in the circuit-switched voice context.

- Even as the project focuses on platforms at sea the requirement for wireline connections through the router has to be included for operation when in port/buoy.

Specific areas of concern for the connectivity with the terrestrial infrastructure are:

- Identification of routes from the command center to the WAN termini. The WAN termini include GSM radio stations, HF receiving stations, satellite earth stations or the PBX infrastructure terminal offices which are connected to the router(s) of the command(s) that provide internet connectivity. Use of VSAT satellite connections is a viable alternative for routing. VSAT satellite connections have been implemented in Bosnia supporting the IFOR operations. (Naval Satellite Communications Functional Requirements Document, 1996) The terrestrial infrastructure support does not have the same critical importance as the radio component, mainly because the availability, reliability and capacity of the terrestrial component are beyond any challenge in traffic the radio component could provide. However, as Buddenberg suggests: "over-buying the terrestrial net will make the ship-shore problem easier."
- Capacity planning for the above routes. However, it should be re-emphasized, availability and survivability are the critical requirements. (Buddenberg, 1993)

- Security for such a network should include a broad planning scope (i.e. need for network management security, authenticity, confidentiality, electronic mail security, security against access and service threats)

3. Services and applications

The following functionality is expected by a network as the one appearing in Figure :

- It must be able to incorporate different radio, cellular, LAN and WAN sub-networks. Physical layer connectivity should be transparent to the information user. Operational or doctrinal considerations (such as the usage of HF or satellite transmissions) must be incorporated in the decision making application which selects the appropriate communications channel from the pool of available connections that support the requirements of transmission (QoS, operational) in the most efficient manner. Network planning and architectural considerations have to ensure that a selection is feasible at all times.
- The protocol architecture of the various sub-networks must ensure interoperability and exchange of information in various data forms among the individual units of the mesh net. The communications requirement for standard operating procedures has not disappeared. Rather, it has been extended to include new data and process types.
- The network must have the capability to dynamically be reconfigured, dependent on the tactical situation. Assumptions for the topology of the network can not be made a priori. Although careful consideration is required with internet routing procedures, they are more easily implemented than earlier changes in communications plans and

do not involve the users of information in the process. However, the increased flexibility may impose a greater burden on doctrine and training. Since there are many more options to choose from in identifying the "optimal" configuration, operational level planners need to be able to distinguish the pros and cons of each configuration.

- Integration of information suppliers and information consumers in a single dispersed mesh has a synergistic effect in knowledge production as the CBE concept discussed in Chapter II suggests. C2 flows of information are expected to be facilitated by such a network in the following areas: (1) intra-ship (2) intra-group (3) shore-ship or shore-group. Also connectivity of Navy units with the commercial infrastructure will facilitate tasks ranging from news coverage to public relations.
- Testing and research based on the project will provide the support basis for expanding and maintaining the network.

4. Doctrine, training and support

Transition from the current concept of communications to the one envisioned by the SeaNet project requires for the Hellenic Navy re-training of existing communications personnel and provision for new subspecialties for day-to-day operation of the system. Considering "network management" as a concept incorporating "whatever it takes to ensure that information workers have access to the information they need, when and where they need it through the network" (Grenier and Metes, 1992) one can not escape the need to connect leadership and network management functions. Doctrine, training and support must be able to provide "whatever it takes".

The following figure shows a multi-dimensional approach to the open questions resulting from the need to connect organizational management (leadership) to information systems management. Again, unity of purpose is the "metric" for success of the management scheme.

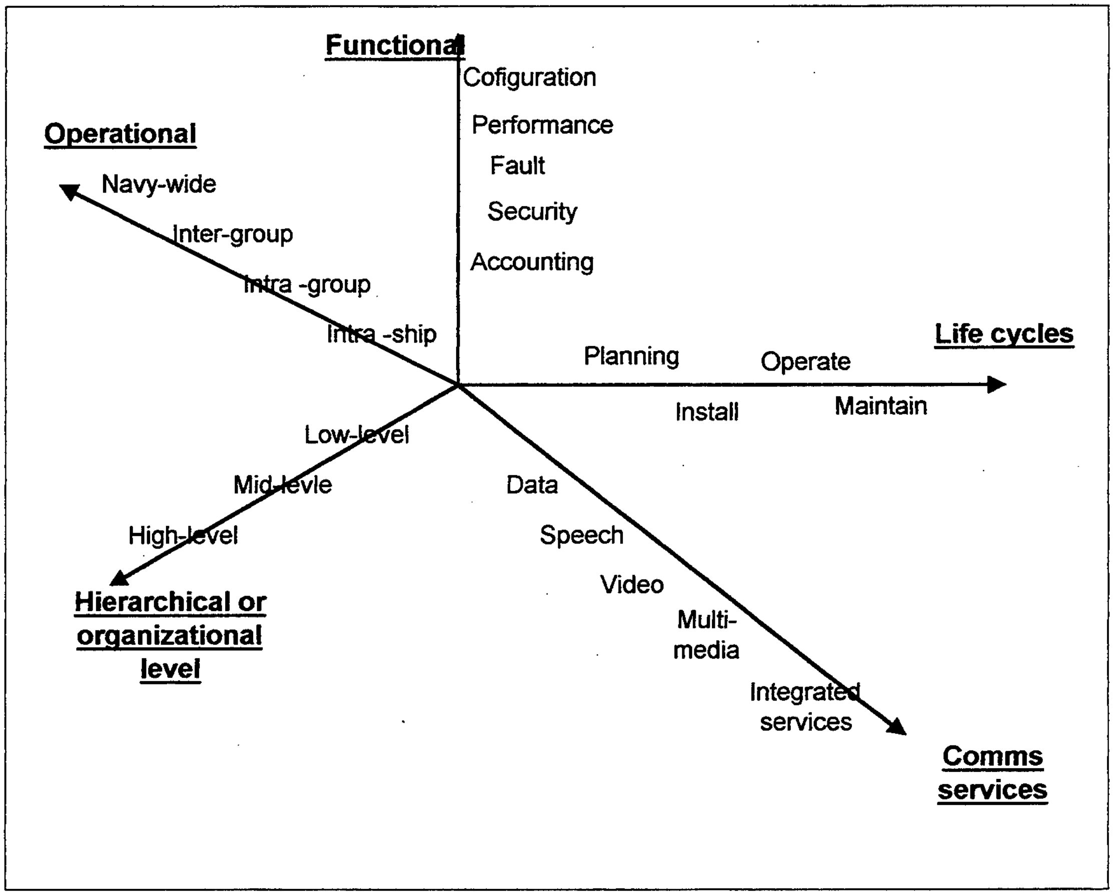


Figure 16. Management and operations dimensions (After Hegering and Abeck, 1994)

The alternative space of options for promulgating doctrine, institute training and provide support is the set of points in the five-dimensional space which relate the variables to each other. And at the meta-level, management becomes the question of establishing a

way to identify, evaluate that alternative space, decide the optimal "volume of points", and finally implement it.

An example is proper to show the utility of the figure above. For military networks, the function of fault isolation is an ability that needs to be developed in-house for all levels of operational networks, reflecting requirements for hierarchically low-level network managers to be trained in the function. In contrast, maintenance of a navy-wide accounting system could be out-sourced, if that is a rational economic alternative. The organizational questions arising from explorations in the alternative space of network management configurations is beyond the scope of the present thesis.

IV. PILOT PROJECT FOR HF E-MAIL AT SEA

A. BACKGROUND ON HF DATA COMUNICATIONS

1. HF Band and data communications

High frequency (HF) radio has been the primary intra-task force medium for ranges beyond line-of-sight, as well as a back up for satellite connections (DREO, 1996). HN, not having a satellite capability apart from limited Inmarsat stand-alone units, relies mainly on HF for its shore-ship and ship-to-ship long-range communication needs. However, the HF part of the spectrum is not conducive to data communications for the following reasons:

- Bandwidth limitations. The spectrum is limited from 3 to 30 MHz, and the channels are three kHz wide. Signaling speed therefore is much lower than the speed observed in wireless LANs. Shannon's law prescribes that for a communications channel with a bandwidth of B Hz, the maximum data rate that can be transmitted and received with no error is given by $C=B\log_2(1+S/N)$, where C is measured in bits per second and S/N is the band-limited signal-to-noise ratio. (Maslin, 1987) To achieve higher throughput we must find ways either to enhance S/N through forward error detection and correction, or use special modulation techniques involving parallel data transmission with multi-tone techniques (Maslin, 1987).
- On a single channel (physical link) there can be only one-way information exchange at a given time (half-duplex operation). (Buddenberg, 1995) Despite this fact, we still experience the "hidden terminal" problem, where one station does not sense that the

channel is occupied and attempts to use it. To resolve similar problems in the wireless LAN world, Bharghavan implemented the MACAW (medium access collision avoidance) medium access protocol, by setting special acknowledgement sequences and back-off algorithms as well as by devising a way to exchange information about congestion among nodes. (Tanenbaum, 1996) Polling is also suggested as a way to increase throughput. (Buddenberg, 1995) The simulation described in Section C, compares results obtained by implementing different link access methods.

- High noise levels. Bit error rates of 10^{-4} are not uncommon for HF channels. (Buddenberg, 1986) In HF channels, noise is the aggregated result of thermal, atmospheric, man-made and galactic noise. In man-made noise, it is important to include EMI effects, given the collocation of electromagnetic emitters aboard a ship or an aircraft. (Maslin, 1987) The high and variable noise levels can be addressed by forward error correction coupled with a "judicious acknowledgement system" (Buddenberg, 1995)
- Interference. Interference is attributed to foreign transmissions at the same frequency, even at great distances from our own site. It includes attempts for transmission within our WAN. (Buddenberg, 1995)
- Specifically for the Hellenic Navy, its area of operations falls to a large extent within the intermediate range in HF communications, where a "silent zone" between ground wave and the skip distance of the first sky-wave exists. Frequency management could address the issue by automatic link establishment techniques (ALE) techniques (Kim et. al., 1995), or by a network topology making use of relay services. Another

possible solution is the use of nearly vertical incident sky waves. (NVIS). (Maslin, 1987)

- The susceptibility of HF communications to interception, jamming and direction finding can be minimized by various techniques, however HF still poses significant security challenges for military operations. (DARPA, 1996)
- Protocols have not matured for HF data communications. Half-duplex operation and inefficient media access have not been addressed with standards. Also, even though multicast protocols are essential to military HF communications since bandwidth is limited and hierarchies tend to exploit best multicast routing schemes, there are no standardized industry-level multicast protocols. DARPA, one of the primary researchers in HF packet radio, states as one of the challenges for HF data communication the development of congestion algorithms, adaptive network routing and end-to-end protocols. (DARPA, 1996) Table 2 relates radio WAN challenges for protocols with the OSI reference model.

OSI Layer	Challenges
Application	QoS, multicasting, connectionless protocols
Session	QoS negotiation
Transport	Variable QoS, selective ACK, reliable multicast
Network	Efficient multicast
Data link	Media access control
Physical	Optimized forward error correction

Table 3. Protocol requirements for radio WAN

Specifically for IP routing, RFC 1677 (August 1994) includes the following requirements for the OSI level 3 (network layer) to support tactical RF systems:

- *Scaling.* The need to achieve a compact addressing scheme for bandwidth efficiency competes with the requirement for unique addressing for every node in the network. That includes SNMPv2 managed devices such as radios or routers. IPv6 supports 10^{12} nodes but address management is still a concern. For our project, two different addressing schemes were implemented since both AX.25 packets and TCP/IP packets used their own addressing. (see below Section B)
- *Connectivity* with other networks and avoidance of stovepipe systems. By utilizing IP, an open standard, internetworking is easier to achieve.
- *Security* at the network layer. Besides any link layer security mechanisms that should protect from denial of service attacks and traffic analysis monitoring, network security considerations include routing protocol authentication, source authentication and confidentiality. Since bandwidth is limited, redundancy of network layer with transport layer security mechanisms should be avoided.
- *Mobility.* The RF network should allow for dynamic topologies. The pilot project allows for UHF, VHF and HF channels utilization, so physical layer connectivity should ideally be transparent to the user, and users will move from one net to another frequently. (see below Section B) Subnets within a net also suggest two different mobility scales. Users moving not only from subnet to subnet but within their own subnet, as well.

- Flows and *resource reservation.* To allow for congestion avoidance of the limited resource (bandwidth), special QoS indicators have to be established. RFC 1677 proposes to include those in the Ipv6 "Type of Service" field. (Adamson, 1994)
- *Multicast* "[is] the general case for information flow in a tactical internetwork" (Adamson, 1994)
- *Policy based routing* and *quality of service routing* allow for prioritization and transport control of individual packets. In NATO's communication system interoperability network (CSNI) project fifteen different packet priorities were envisaged. (Adamson, 1994)
- *Datagram service.* The memory provided by the datagram enhances survivability in dynamic topologies.

Along the same lines, the Australian Defense Communications Research Centre of the Signal Processing Research Institute in Adelaide, has developed a number of postulates from research on HF tactical packet networks. They include the recognition for a needed unique addressing scheme across the network, a self-organizing capability for the network, stand-alone operation and the need for protocol unification. (DCRC, 1996) Despite the above mentioned challenges, HF data communications are receiving again much attention due to the high cost of satellite connections and advancements in microprocessor computing power which allows implementation of adaptive techniques and fast serial modulation with error control(Maslin, 1987). Packet radio technology has been one of the significant contributors to the renewed interest for HF.

2. HF Packet radio

Data packet technology was developed in the mid 1960s by ARPA. Alohanet was the first radio based (407,350-413,475 MHz) large scale project in 1970 with a speed of 9600 bps. The amateur radio community has experimented since the early 1980s with digital data transmission, which resulted in the standardization of a communications protocol for packet exchange between radios for the link OSI layer (layer 2). It is based on the wired X.25 and is called Amateur X.25 or AX.25. AX.25 frames are sent synchronously in HDLC frames. A worldwide amateur packet radio network exists today (AMPRNET) supporting TCP/IP protocols and providing access to the Internet[3], based on the KA9Q internet protocol package (Karn, 1987). Packet radio technology offers transparency, error checking, automatic control and longer range networking through relaying nodes (digipeaters) which made it favorable among other digital modes. Furthermore, it offers resilient networks since failure of one node will not bring down the complete network. Significant for military applications, it also offers mobility and easy deployment. Its most important limitations are those of the HF medium it utilizes and have been addressed above.

Research on packet radio is far from over however. Besides the presently reviewed project undertaken by NRaD, DARPA also in the United States, is engaged since 1983 in the SURAN program (survivable, adaptive networks) to research and develop technology capable of supporting communications between computers and their users in the modern battlefield. (DARPA, 1996) The Canadian Defense Research

[3] In Greece, there is an active and growing body of amateur radio enthusiasts. (Zachariou, 1996) The AX.25 addressing scheme for Greek stations is: 44.154.x.x

Establishment in Ottawa (DREO), has developed an adaptive HF terminal. Its adaptive features include a real time channel evaluation and selection mechanism, an adaptive link protocol for channel optimization and a fully distributed and adaptive routing algorithm for the selection of routes within an HF network. (DREO, 1996) The Australian Defense Force is conducting research on the use of HF in self-organized, mobile, packet radio networks and in their integration with the overall military communications infrastructure. Within NATO, integration of different media to seamlessly provide services for NATO commands and forces, is being researched in the CSNI project.

B. THE NRAD BATTLE FORCE E-MAIL PROJECT

1. Background and features

"*Battle force electronic mail*" has been the result of research conducted by the Naval Command, Control and Ocean Surveillance Center, RDT&E Division (NRaD) of USN, in San Diego. It provides secure, error-free automatic delivery of e-mail messages, and binary files such as images and graphics. (Danielson, 1996) The amateur packet radio network operating system JNOS is used after it was modified to ensure interoperability with cryptographic devices such as the KG-84C. The system has been tested across HF, UHF, UHF DAMA satellite, EHF satellite and the VHF SINGARS radio system as well. A basic block diagram of the system is shown as Figure .

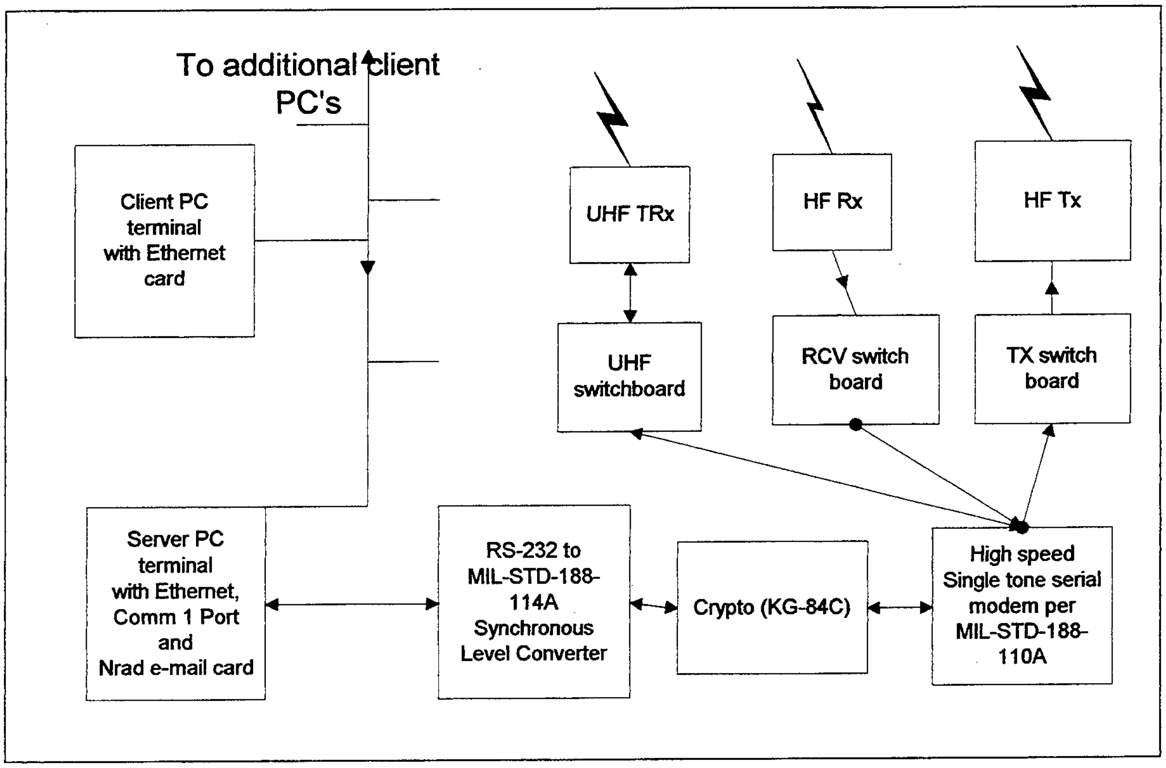


Figure 17. Battle Force E-Mail Block diagram. (From Danielson, 1996)

The system has been deployed in three different modes. The ship-to-ship configuration has already been installed (September 1996) in four carrier battle groups and two amphibious ready groups. (Danielson, 1996) Successful implementation of the ship-to-ship mode resulted in a ship-shore experiment involving a submarine, USS Dolphin, which conducted transmissions in ranges of up to 1250 miles. Automatic mail delivery and Internet access were provided to the submarine through the NRad mail server and router in San Diego. The third mode, air-to-ground HF connectivity, was tested with a C-130 Speckled Trout airplane that utilized an ALE (MIL-STD-188-141A) modem

controller which allowed the airplane to maintain HF connectivity at 1200-2400 bps with the NRad site continuously in a cross-continent flight[4]. (Greer, 1996)

We view the system as being built --after our discussion in Chapter III-- of the following sub-systems:

- Shipborne LAN, which is an Ethernet LAN in most cases. The LAN is used to connect the client PC with the server via standard SMTP or POP3. The server supports all the usual server functions as well as external connections via RF media and landline connections. In the HN HYDRA class frigates such an Ethernet exists with built-in redundancy (reliability-availability) features. It provides connectivity between the radio communications server and users in various departments aboard the ship.
- Radio subsystem, better termed subnet (or radio-WAN segment) after the discussion in Chapter III, which comprises of the radio equipment, modems, cryptographic devices and the serial communications equipment as well as their interfaces. In the NRad project the implementation of a unique PC card was necessary to ensure timing control for the radio equipment along with serial port support and hardware flow control for the PC side. (Danielson, 1996) Implementation of the project using ALE compliant radios allows for less human supervision and monitoring of the radio subsystem, an important consideration for small ships. The HF modem has to support the single tone serial waveform per MIL-STD-188-110A. It is a robust waveform and can support speeds up to 4800bps. In the cases where multipath phenomena are not severe 9600bps could be reached. (Danielson, 1996) However, modem performance

[4] The cost of equipment for the test was less than $16000 (Greer, 1996)

is less robust and user data becomes corrupted. The trade-off between physical layer performance in speed and forward-error correction methods must be emphasized. The only *radio* requirement is a stable 3.0 kHz waveform.

- Communications software, which includes the JNOS software and the e-mail client/server communications, package. JNOS is a multitasking (many sessions can be run in parallel), DOS-based network operating system, which supports both the most commonly used internet protocols such as TCP, IP, TELNET, FTP, SMTP, plus the packet radio protocols AX.25, NET/ROM and PBBS mail. (Wade, 1996) The basic requirements to run JNOS are: a PC; a copy of the NOS software --available as shareware-- and an Internet address. JNOS offers the capability for chats (whiteboards), remote login, file transfers and mail transfer. The requirement for dual addressing (IP and AX.25) is resolved by a local DNS-like service. Serial interface to the modem is through the serial communications card and an RS-232 connection. The client communications package is the commercially available Eudora package, even though any SMTP supporting package would perform.
- People. Successful deployment of any pilot project is depending on the users and their inputs to define the limits of the system. Furthermore, an educational aspect is present here as this project could introduce new ways of communicating for the teletype bound Hellenic Navy.
- Procedures. The need to establish standard operating procedures for the use of "battle force e-mail" is important, especially since the underlying link access implementation (CSMA) gives a non-hierarchical "fairness based" access to the HF channel.

2. User data encapsulation

The protocol stack for the specific implementation starting from the user's data is as follows (see Figure 17):

- User or system file. Data is in ASCII format. Attached files to the e-mail message are all ASCII and they are passed as such to the communications server.
- Simple Mail Transfer Protocol (SMTP). It provides the necessary interface for TCP to access the server mail directories and handles the forwarding and reception of the mail.
- Transport Control Protocol (TCP). It breaks mail files into data packets (e.g. 256 bytes each including 32 bits of overhead) and handles end-to-end (i.e. across multiple net segments) acknowledgements (ACK) or negative acknowledgements (NACK). Since it is a connection-oriented protocol, it establishes virtual circuits between stations for flow control and recovery. The nature of the HF medium requires a careful setting for time-outs. The nature of transmitted data on the other hand, requires that the error recovery method is flexible. Image data should sacrifice accuracy for speed, where transmission of a detailed op-order can not afford a mistaken set of coordinates. Duplication of error control with the link layer is also a concern. UDP transmission could be a viable alternative if robust error detection and correction is achieved at the link layer.
- Internet Protocol (IP) It contains routing information.
- AX.25. The AX.25 protocol includes its own addressing scheme, as well as the framing for subsequent radio transmission.

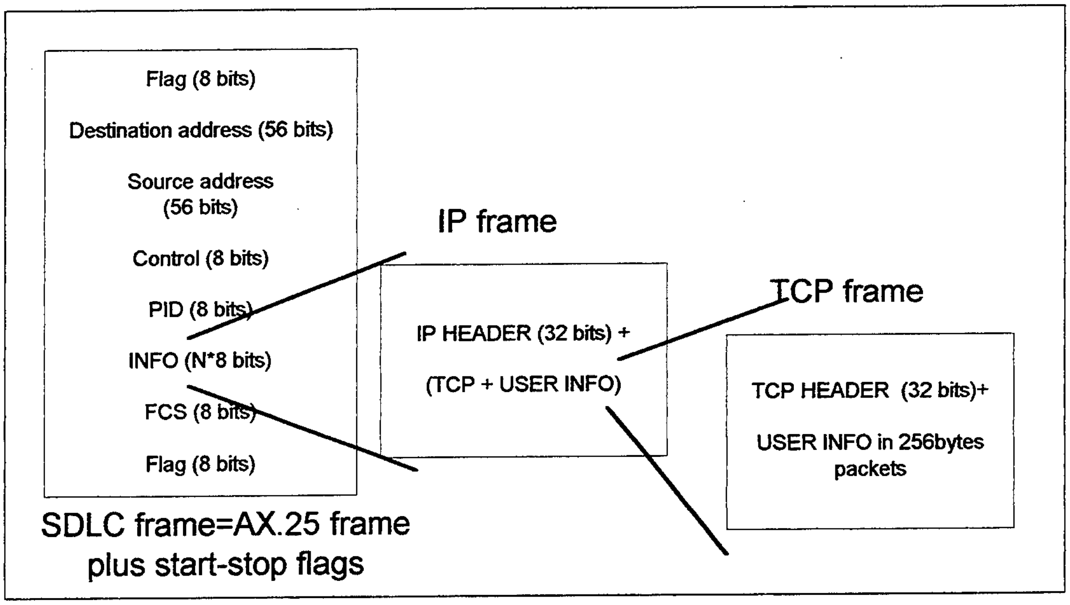


Figure 17. Encapsulation of user data in TCP-IP-AX.25 frames (After Danielson, 1996)

- Synchronous Data Link Protocol. Industry standard, its framing is applied and removed by the serial communications board.

The total overhead for a user data packet of 256 bytes is 19 bytes including TCP, IP, AX and SDLC encapsulation. Transmission over the air is made using a CSMA link access discipline with separate queues for every potential net participant. (Danielson, 1996) Thus, the server will not delay transport of messages to other participants if one of them is not reachable. In addition, CSMA makes all participants equal, so that there is no dependence on one node for network control. Different networks require only different frequencies.

3. Potential applications

Electronic mail with ASCII attachments is the primary application of the "battle group electronic mail." The ability of JNOS however, to support different services, its physical layer independence and the open nature of employed protocols, as well as the diversity of operational environments in which it can be used, make the project a valid candidate for *the* prototypical application in the transition the HN has to make to seamless information systems. It can support whiteboards in ad hoc virtual conferences among commanders. Its use in emergency relief operations could also be of significant value, since other communications infrastructure might be unavailable. It is also suggested by its developers that it will host the Defense Messaging System e-mail application as a tactical terminal in the "near future" (Danielson, 1996)

HF-email is a true Internet system since it uses the TCP/IP suite. Thus, any internet application --subject to bandwidth limitations-- works over the HF radio network. The configuration also allows HF to be adapted to the router-based Internet. That, makes the HF channel one *of a non-mutually exclusive pool* of physical media that can be utilized to connect the various end nodes (sense-decide-act) into the network for exercising command and control.

C. THE PROJECT AS PART OF THE TRANSITION TO A NEW ARCHITECTURE

After the discussion in Chapter III, for the network centric and information conducive architecture that HN has to develop, the "battle force e-mail project" appears as a significant part of the transition process. Bibliography suggests rapid prototyping as a useful method to assist transition in information systems, mainly because of immediate user involvement and minimal time lags between planning and execution. (Spewak, 1993 and Guengerich et. al., 1997) The reviewed system is considered as a successful prototype to use in the transition that has been the muse of the present thesis.

Benefits from its implementation appear to be the following:

- It will enhance the *operational capabilities* of units and commands by allowing faster data exchange as well as information exchange in different formats (text, image, audio, whiteboards). It will also provide for data communications diversity by being a viable alternative to satellite connections. It will also allow HN to accomplish more efficiently possible civil disaster operations or operations other than war.
- It is of *minimal cost* to implement, it has already been tested and it uses available and *open standards*. It is a non-stovepipe system, capable of integrating with both the wired (PBX) and wireless (cellular) information infrastructure through its JNOS connectivity.
- It will involve command, control and communications teams during its exploitation and will therefore act as a *training* experience in traditional issues such as security, reliability and speed but with an "information age" flavor.

* It will support development for *shipborne LANs* beyond the already existing ones in the HYDRA class frigates, with obvious benefits.
* It can utilize previous communications projects undertaken by HN, such as AMPS[5], thereby *minimizing its deployment costs* and any previous sunk costs by using already existing PC equipment.
* It will show the *needs in personnel* of particular expertise to operate and manage information systems.
* It will help in assessing *procedures and policies* promulgated at the national level for information warfare.
* It will *facilitate interoperability* between HN units and other NATO naval units which posses similar capabilities.

A future scheme for HF packet radio integration into the C2 network is shown below:

[5] Automatic Message Processing System.

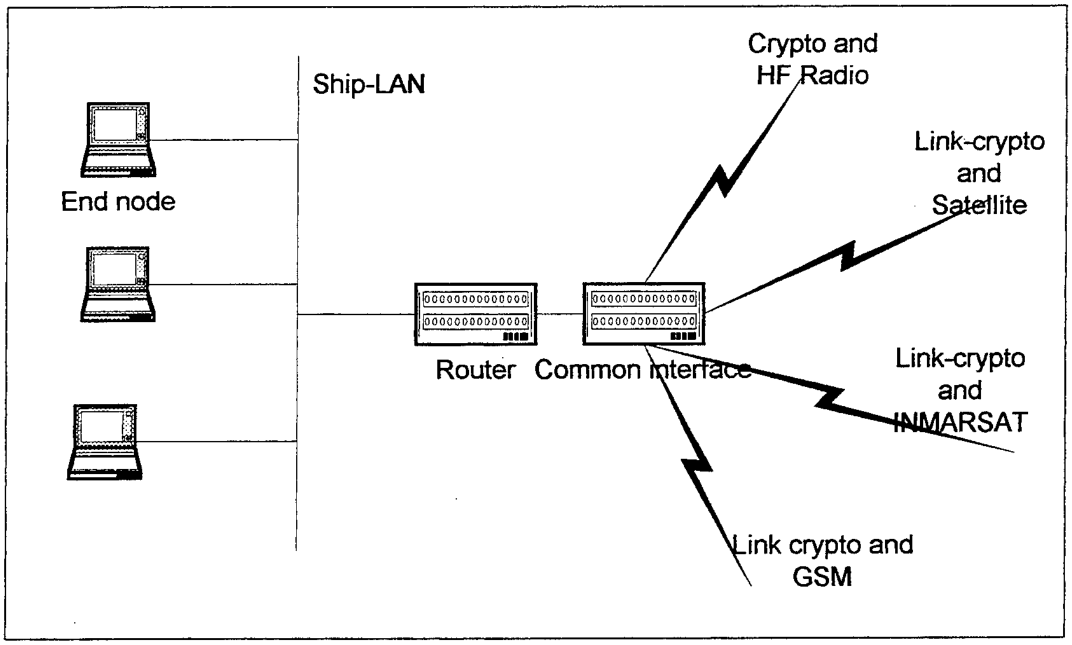


Figure 18. Future vision of radio-WAN link connectivity for a mobile platform

D. SIMULATION WITH COMNET

COMNET is a graphical, off the shelf package that allows you to conduct performance analysis for computer and communications networks through simulation. Based on a description of the network, its control algorithms and workload, COMNET simulates the operation of the network and provides measures of its performance. Our simulation aimed primarily to better acquaint us with an HF packet radio network similar to the one employed by "battle force e-mail," through the development of the necessary simulation parameters. It has been used therefore as a training tool. A secondary benefit has been the examination of performance parameters in different HF packet-based networks.

The network built was comprised of ten stations or nodes, representing ten ships. All simulation characteristics for every run (four runs of 10150 seconds each) appear in Appendix C. Each node was both receiving and contributing traffic to the network. Traffic size was simulated as following a normal distribution for all ships, with a mean of 50 kilobytes (KB) and one standard deviation. The command ship was contributing 100KB messages to the network. Message sizes were chosen after considering that the current AUTODIN average message size for text only messages is two thousand five hundred bytes. (Morales, 1996) Message inter-arrival times 2700 seconds reflecting 32 messages transmitted per day per station as 32 has been the theoretical limit for channel utilization obtained by M/M/1 queue theory for exponential arrivals for such traffic. (See Appendix C) The above traffic characteristics were held constant through all runs.

The transport protocol simulated was TCP and the packet and framing characteristics that were used reflected the data encapsulation scheme in "battle force e-mail." Depending on the available bandwidth two different frame lengths emerged: 511.66 msec (4800 bps) and 255.83 msec (9600 bps), all modeling 307 byte frames (256 user + 40 TCP/IP overhead +11 AX.25 overhead). Four different options were examined for link access: CSMA at 4800 bps, CSMA at 9600 bps, polling at 4800 bps with a control channel available and polling at 4800 bps without control channel availability[6]. The characteristics for propagation delays were kept constant in all runs simulating a distance between the end nodes in the network of 200 nautical miles (or 1.2 msec).

---

[6] Control channel provides the command ship with one more channel for network engineering traffic.

The metrics analyzed after every run were:

- Received message count (per node and total): It provided a general estimation of the traffic exchanged in the 10150-second simulation. The metric includes only successful receptions of messages.
- Buffer input/output per node. How many bytes have been placed in the input/output buffer of every ship for reception/transmission. Not all of them have resulted in successful transmissions.
- Link utilization. Percentage of the simulation run time the channel was busy. That metric is of operational as well as technical importance, since it reflects the susceptibility of the network to attacks.
- Frames delivered. Actual throughput of the system.
- Average transmission delay. The average delay for successfully transmitted frames.
- Collisions. The number of collisions because of failed contention. Collisions are only occurring in CSMA mode. The number of collisions is a meaningful metric when compared to the number of delivered frames, as a percentage.

Simulation results appear in the appendix for every run[7]. There is an important qualification for the validity of the simulation results. Since the message inter-arrival time has been around 1000 seconds, a run of 10150 seconds is not statistically valid. However, findings still reinforce the primacy of bandwidth in defining network

[7] Results include various computer outputs and graphics. However, for an overview of the simulation a comprehensive table is included at the end of Appendix C

performance. Link utilization at 4800bps has been 85% where utilization at 9600bps was 70%. Both of those numbers appear significantly higher than the theoretically calculated channel utilization. Also important has been the observation that polling as a link access method, making use of the synchronization bits in the AX.25 frames, displayed better throughput characteristics for the network than CSMA. (4607 data frames delivered with CSMA link access while the polling method allowed delivery of more than 9000 data frames). In addition, presence of a control or engineering channel showed a reduction of traffic load on the working one and an increase in throughput. The COMNET simulation runs for the CSMA link access method showed in both the 4800 and the 9600bps cases a saturation of the medium by traffic after 3600 seconds in 4800bps and after 4800seconds in 9600bps.

As a future simulation project the interconnection of packet radio networks or their integration with the terrestrial information infrastructure could be examined. Routing decision-making could also be modeled in those more complex networks. In our simulation, all stations have been in "one-hop" distance resembling a long range LAN rather than a WAN comprised of routers.

V. CONCLUSIONS AND RECOMMENDATIONS

A. GENERAL

The SeaNet model presents a challenging prospect for the much needed modernization of the information infrastructure of the Hellenic Navy. The structured nature of the model allows for a transition phase as it becomes moderated by economic and other organizational constraints such as the lack of in-house expertise. However, to ensure unity of purpose for projects initiated under this transition an information architecture framework is necessary.

The appropriate architectural background has to be developed by realizing the close interrelation between the C2 requirements and the characteristics of the network-centric architectural model for information systems. Integration of knowledge-seeking and knowledge-producing nodes in a seamless, dynamic and resourceful mesh, which has by design high reliability and availability, and offers differentiated qualities of service is the vision of the architecture.

The small-scale pilot implementation of an HF-based "Battle Force E-mail system" shows the potential and is considered a primer for the transition. Nonetheless, issues arising from that project and require further research --if the overall concept is adopted-- are:

- Development of an appropriate interface that allows a shipboard router to intelligently choose the appropriate radio-WAN connectivity given a set of decision parameters.
- Evaluate the currently available components for the constitution of a SeaNet project in Greece.

- Evaluate emerging protocols at the link and transport layers for radio-WAN implementation.
- Develop a methodology for the promulgation of a HN-related information architecture.
- Identify the optimal transition path to a new information architecture for the HN.

The above topics for further research could be used as potential thesis areas for future Hellenic Navy NPS students.

B. RECOMMENDATIONS FOR AN "INTERNET AT SEA" FOR THE HN

This thesis proposes a transition from the current state of information systems to a network-centric architecture for the Hellenic Navy. The transition should involve different command levels across functional areas of the program, following the systems management paradigm depicted in Figure 16. In the following bulleted lists specific recommendations are made for different "stakeholders" in the transition. They emerge from our discussion across the thesis, however, they are collectively presented here as a conceptual guide for action. Key participants in the transition program are considered the following:

- Hellenic Navy General Staff (HNGS)
- Operational Commanders and their staffs (COMHELFLEET)
- Support Commanders and their staffs
- Hellenic Naval War College. The Naval War College should initiate the development of doctrine and tactics for an information warfare environment.

- Research Labs, Academic Institutions
- Greek Telecommunications Industry and Communications Services Providers

The Hellenic Navy General Staff has the budgetary authority required for initiating the program as well as the capability to coordinate the external and internal aspects of the venture. Specifically it is suggested that, the HNGS:

- Initiate a Navy-wide inventory of information systems, business functions and data repositories already in place
- Assign a Program Manager (PM) and a Program Management Team for managing the transition. Provide budgetary, knowledge and human resources to the PM
- Develop a preliminary information architecture vision and the corollary strategies
- Incorporate the Hellenic information technology industrial base into the project. Information systems should be considered under the scope of national security as well. In-country development and support is critical for the transition to the "information warfare age".
- Adopt a set of technical standards after the PM's recommendation for implementation. The focus here, is on the interface among the systems. For example, the hardware interface (Ethernet or FDDI), the enveloping definition (SMTP/MIME), and the SNMP agent are standards that should be requested from vendors on their products, so that they have the qualities of a "good network citizen" (Buddenberg, 1996)
- Acquire conventional terrestrial Internet infrastructure to interconnect the command centers, support centers and other terrestrial information consumers/providers. The routing nodes and the network management sites should be the communications

centers that are already existing. (24-hour support) The criteria of network availability and survivability will be enhanced by developing alternate routes. Connection with the outside world should be considered through Network Access Points (NAP)

- Initiate the revision of training programs and specialty descriptions to satisfy immediate needs in network management. Petty officers should be able to use network management platform software. Radiomen will be transformed to network technical controllers and administrators. However, there is a need to define what an officer of information technology as well as the enlisted will do. One more problem here seems to be the high turn-over rate of enlisted personnel due to the existing draft. The ability of the Hellenic Navy to develop information "warriors" across the hierarchical level will mark its success in the transition.

The operational commanders should:

- Initiate the inventory of existing information systems
- Develop the requirements --as users-- for the new information systems
- Exploit installed pilot-projects (such as the Battle Force e-mail) during exercises and operations, and develop the knowledge base and the expertise for further input into the development of the information architecture.
- Test the doctrine and tactics made available to them and provide feedback. Appendix D is a schematic approach of the doctrine testing function through mission capability packages, suggested by Johnson and Libicki. (Johnson and Libicki, 1995)
- Develop standard operating procedures (SOP) for the information systems aboard their units. The intra-ship and inter-ship part of the network should be under the

direct control of the operational commands for faster development. The ship-shore part of the network has to provide three functions and should be coordinated with shore authorities: (1) In-Navy use for ship-shore traffic(2) Access to external (non-Navy) information sources (3) As an alternate route for shore stations. However, once the terrestrial infrastructure is in place and the shipboard LANs are operational the radio part of the network will be a matter of answering *how* does the Hellenic extend the Internet to sea, rather than *what* does the Hellenic Navy do for ship-shore. (Buddenberg, 1996)

The support commands should:

- Complete the inventory of their information systems
- Develop the requirements --as users-- for the new information systems
- Install on the ships shipboard LANs and the HF e-mail components, as the first step towards extending the Internet-based network to sea
- Develop the knowledge base to support the deployed information systems

The research community within the Navy should:

- Assign resources for exploring improvements for the radio part of the network. Specifically, for research on HF modulation techniques that support waveforms which provide data rates higher than 4800bps, as well as transport and link protocols that are IP compliant while radio-WAN friendly.
- Explore the potential of using the Internet connectivity of units at sea for conducting research

The PM is envisaged as the central point of contact within the Navy for the Internet at Sea Project for the Hellenic Navy.

APPENDIX A. BUDGET ESTIMATE

This appendix shows the estimated budget for the SeaNet project for Years 1 and 2, along with the necessary explanatory notes. (copied from Buddenberg et al., 1996)

BUDGET ESTIMATE

Item	Year1	Year2
Shipboard Equipment and Installation	$535,450	$0
Shipboard communications costs	$412,050	$200,000
Software development/integration	$200,000	$100,000
Central site costs	$99,100	$45,000
Testing, education	$98,100	$20,000
Project management	$96,250	$10,000
TOTAL Direct costs	**$1,381,950**	**$375,000**
Overhead at 25%	$345,480	$78,000
Less cost sharing	-$539,800	$0
Total actual costs	**$1,187637**	**$450,000**

Notes:

- *Shipboard Equipment and Installation* costs vary greatly with the number and type of communication systems employed. In this version of the budget we assume that a pool of 8 INMARSAT-B High Speed Data, 3 cellular telephone systems, 2 AMSAT systems and 2 HF Radio systems will be made available to the fleet A more detailed analysis of the needs of the community may result in a different mix in the final proposal. Some ship operators may also have some of this equipment installed on their ships.
- *Shipboard communications* costs represent a subsidy amount to be put towards user satellite usage and other costs. This pool of money will be used to pay 50% of the communications costs for all ships included in the trial. If fewer communication systems are included in the final proposal this amount will be smaller.
- *Development and integration* costs are related to the work that needs to be done to develop the SCN into a production unit and interface it to two new types of communication links.
- *Central site* costs represent those costs related to operations and user services unique to managing a ship-based internet using non-standard communications links to carry Internet traffic

- *Testing and education* costs will be used to support graduate students and staff at the graduate school who will be exploring more cost effective options for communications in the future and a design review for the system.
- *Project management* and review panel costs are related to the work JOI will be doing to work with the community to determine which research programs can best use the communications systems and to closely coordinate the SeaNet efforts with UNOLS activities.
- *Cost sharing* arrangements are still being discussed among the partners. To date, COMSAT has offered a discount in its normal INMARSAT-B HSD rates. Omnet has offered to waive the 25% overhead charge and WHOI has contributed new equipment and software for the software development effort. Discussions with other partners are under way

APPENDIX B. GSM COVERAGE IN GREECE

Below is a map depicting coverage of cellular services in Greece as they have been in January 1997. Even though there has been an expansion of the coverage the last years, GSM connectivity is not assured for large areas of the Aegean and therefore will be of limited value to the network. (Map downloaded from: http://www.panafon.gr/wwwpage/cov_map.html)

APPENDIX C. SIMULATION DATA

In the following tables, simulation results from operation of a packet radio network over an HF channel appear. It consists of 10 ships each contributing the same traffic load to the network. Tables 2-5 are theoretical approximations using queue theory for various parameters of traffic load. Table 2 represents the case where each ship contributes 32 ships of 50K length at 4800bps bandwidth. From this starting point we changed the message length (100K), the number of messages per ship (85) and the available bandwidth (9600bps) to construct the other tables. In approximating the wireless LAN, we assumed frames of 307 bytes (256 user bytes plus layer two and above overhead) and included TCP end-to-end acknowledgments in our calculation. The queuing calculations were made for a M/M/1 model (Kendall notation). The Lq, Ls, Wq, Ws data were inserted to the tables after we used a production management software package. (POM software-copyright, 1996 Howard, Weiss) to find their values. The objective has been to theoretically estimate the:

- Percent utilization of the channel, and the
- Queue and service lengths,

in order to make comparisons with the COMNET simulation results.

Pages 89-99 are the simulation results obtained by COMNET for the following conditions:

- 10 ship network with 32 messages per ship per day, at 4800bps using CSMA as the link access method (Battle Force e-mail)

- 10 ship network with 32 messages per ship at 4800bps using polling as the link access method without a control channel.
- 10 ship network with 32 messages per ship at 4800bps using polling with a control channel (4800bps) for traffic engineering.
- 10 ship network with 32 messages per ship at 9600bps.

The data entered in COMNET appear in the following table for all four simulations:

	4800 CSMA	***4800 Polling-no con***	***4800 Polling-w/con***	***9600 CSMA***	***Notes***
#Ships	10	10	10	10	
#Messages/ ship/day	32	32	32	32	
Message interarrival time (cmd)	1900	1900	1900	1900	seconds
Message interarrival time (ship 2-9)	2700	2700	2700	2700	seconds
Message size (cmd)	102400	102400	102400	102400	bytes
Message size (ships 2-9)	51200	51200	51200	51200	bytes
Bandwidth	5	5	5	9.6	kbps
Collision window	0.6	na	na	0.6	msec
Interframe gap	0.2	na	na	0.2	msec
Propagation delay	1.2msec	1.2msec	1.2msec	1.2msec	200 n.miles
Frame min.	51	51	51	51	bytes
Frame max.	307	307	307	307	bytes
Frame OH	11	11	11	11	Bytes
Frame error p	0.00015	0.00015	0.00015	0.00015	probability
Run-time /warm-up	10150 /1000	10150 /1000	10150 /1000	10150 /1000	sec/sec
Control channel	na	No	Yes(4800)	na	-------

Table1. Used COMNET simulation parameters

Number of ships	10 ships
Messages per ship	32 messages/day
Message size	50120 bytes
total user bytes	16038400 bytes
Bandwidth available	4800 bps
Packets user (256bytes)	62651 packets
TCP/IP overhead	40 bytes per packet
Layer 2 overhead	11 bytes per packet
Total bytes to be Xmited	16728257 bytes
Total number of frames	54490 frames
TCP ACK frames	6811.25 frames
Bits Xmit for ACK	2179600 bits
Total bits	136007040 bits
Interframe gap	0.0002 sec
Propagation delay	0.0012 sec
Total service time	28419.2593 sec
Ratio of 24hours	0.328926612 average link utilization
Lamda	0.00037037 transactions/second
Mu	0.001125997
Av. number in queue (Lq)	0.1612 messages
Av. number in system(Ls)	0.4902 messages
Av. time in queue (Wq)	435.3092 sec
Av. time in system(Ws)	1323.417 sec

Table 2. HF Packet radio LAN simulation with M/M/1 queue and 50K message size at 4800 bps and 32 messages per ship

Number of ships	10 ships
Messages per ship	32 messages/day
Message size	102400 bytes
total user bytes	32768000 bytes
Bandwidth available	4800 bps
Packets user (256bytes)	128001 packets
TCP/IP overhead	40 bytes per packet
Layer 2 overhead	11 bytes per packet
Total bytes to be Xmited	34176707 bytes
Total number of frames	111325 frames
TCP ACK frames	13915.625 frames
Bits Xmit for ACK	4453000 bits
Total bits	277867200 bits
Interframe gap	0.0002 sec
Propagation delay	0.0012 sec
Total service time	58061.55355 sec
Ratio of 24hours	0.672008722 average link utilization
Lamda	0.00037037 transactions/second
Mu	0.000551139
Av. number in queue (Lq)	1.3884 messages
Av. number in system(Ls)	2.0618 messages
Av. time in queue (Wq)	3748.817 sec
Av. time in system(Ws)	5566.999 sec

Table 3. HF Packet radio LAN simulation with M/M/1 queue and 100K message size at 4800bps and 32 messages per ship

Number of ships	10 ships
Messages per ship	82.69592082 messages/day
Message size	50120 bytes
total user bytes	41447195.52 bytes
Bandwidth available	4800 bps
Packets user (256bytes)	161904 packets
TCP/IP overhead	40 bytes per packet
Layer 2 overhead	11 bytes per packet
Total bytes to be Xmited	43228808 bytes
Total number of frames	140811 frames
TCP ACK frames	17601.375 frames
Bits Xmit for ACK	5632440 bits
Total bits	351464256 bits
Interframe gap	0.0002 sec
Propagation delay	0.0012 sec
Total service time	73439.97685 sec
Ratio of 24hours	0.849999732 average link utilization
Lamda	0.000957129 transactions/second
Mu	0.001126034
Av. number in queue (Lq)	4.8167 messages
Av. number in system(Ls)	5.6667 messages
Av. time in queue (Wq)	5032.417 sec
Av. time in system(Ws)	5920.489 sec

Table 4. HF Packet radio LAN simulation with M/M/1 queue and 85% utilization at 4800bps (82 messages per ship of 50K each)

Number of ships	10 ships
Messages per ship	82.69592082 messages/day
Message size	50120 bytes
total user bytes	41447195.52 bytes
Bandwidth available	9600 bps
Packets user (256bytes)	161904 packets
TCP/IP overhead	40 bytes per packet
Layer 2 overhead	11 bytes per packet
Total bytes to be Xmited	43228808 bytes
Total number of frames	140811 frames
TCP ACK frames	17601.375 frames
Bits Xmit for ACK	5632440 bits
Total bits	351464256 bits
Interframe gap	0.0002 sec
Propagation delay	0.0012 sec
Total service time	36829.11685 sec
Ratio of 24hours	0.426262927 average link utilization
Lamda	0.000957129 transactions/second
Mu	0.002245395
Av. number in queue (Lq)	0.3167 messages
Av. number in system(Ls)	0.743 messages
Av. time in queue (Wq)	330.8812 sec
Av. time in system(Ws)	776.2371 sec

Table 5. HF Packet radio LAN simulation with M/M/1 queue at 9600bps for the same traffic load as Table 3 (82 messages per ship of 50K each)

4800 CSMA

INPUT BUFFER USE BY NODE

REPLICATION 1 FROM 1000.0 TO 11150.0 SECONDS

	Packets accepted	Packets blocked	Average Buffer use (bytes)	STD DEV	MAXIMUM
SHIP1	400	0	0	0	3
SHIP2	271	0	0	0	15
SHIP3	778	0	0	0	296
SHIP4	601	0	0	0	296
SHIP5	401	0	0	0	296
SHIP6	416	0	0	0	296
SHIP7	350	0	0	0	296
SHIP8	307	0	0	0	296
SHIP9	1047	0	0	0	296
SHIP10	602	0	0	0	296

OUTPUT BUFFER USE BY NODE

	Packets accepted	Packets blocked	Average Buffer use (bytes)	STD DEV	MAXIMUM
SHIP1	408	0	550	996	2368
SHIP2	271	0	747	1097	2368
SHIP3	818	0	6451	5663	14208
SHIP4	625	0	2949	3092	7104
SHIP5	425	0	3103	3149	7104
SHIP6	424	0	1284	796	2368
SHIP7	390	0	5383	4329	11846
SHIP8	323	0	2453	2338	7104
SHIP9	1063	0	2303	2220	4736
SHIP10	610	0	306	773	2383

RECEIVED MESSAGE COUNTS 4800 CSMA

RECEIVER	*COUNT*
SHIP 3	2
SHIP 4	2
SHIP 5	1
SHIP 6	2
SHIP 9	4
SHIP 10	1

Total received: 12

LINK DELAYS AND UTILIZATION 4800 CSMA

LINK	Delivered frames	Resent Frames	Average Delay	Maximum Delay	Utilization %
HF Packet 4800 CSMA	4607	12	781.844	78593.400	84.95

RANDOM ACCESS LINK PERFORMANCE

4800 CSMA

LINK NAME	*HF PACKET 4800 CSMA*
COLLISION EPISODES	354
COLLIDED FRAMES	46277
# TRIALS TO RESOLVE (AVG)	2.87
# OF DEFERRALS (AVG)	1448
DEFERRAL DELAY (MS) -(AVG)	467.21
DEFERRAL QUEUE SIZE (FRAMES)	0.07
MULTIPLE COLLISION EPISODES	308

9600 CSMA

INPUT BUFFER USE BY NODE

REPLICATION 1 FROM 1000.0 TO 11150.0 SECONDS

	Packets accepted	Packets blocked	Average Buffer use (bytes)	STD DEV	MAXIMUM
SHIP1	1001	0	0	0	296
SHIP2	600	0	0	0	296
SHIP3	1389	0	0	0	296
SHIP4	217	0	0	0	296
SHIP5	1011	0	0	0	296
SHIP6	601	0	0	0	296
SHIP7	617	0	0	0	296
SHIP8	286	0	0	0	300
SHIP9	579	0	0	0	296
SHIP10	687	0	0	0	296

OUTPUT BUFFER USE BY NODE

	Packets accepted	Packets blocked	Average Buffer use (bytes)	STD DEV	MAXIMUM
SHIP1	1025	0	1341	2089	7104
SHIP2	608	0	699	1079	2368
SHIP3	1421	0	4851	4853	11840
SHIP4	241	0	2932	3104	7107
SHIP5	1035	0	3070	3170	7104
SHIP6	601	0	17	191	2368
SHIP7	649	0	3472	3505	9176
SHIP8	294	0	839	1761	4736
SHIP9	595	0	2258	2245	4736
SHIP10	695	0	254	727	2368

RECEIVED MESSAGE COUNTS 9600 CSMA

RECEIVER	*COUNT*
SHIP 1	1
SHIP 2	2
SHIP 3	3
SHIP 5	4
SHIP 6	2
SHIP 7	1
SHIP 9	1
SHIP 10	2

Total received: 16

LINK DELAYS AND UTILIZATION 9600 CSMA

LINK	Delivered frames	Resent Frames	Average Delay	Maximum Delay	Utilization %
HF Packet 9600 CSMA	6720	13	331.140	37864.733	69.30

RANDOM ACCESS LINK PERFORMANCE

9600 CSMA

LINK NAME	*HF PACKET 9600 CSMA*
COLLISION EPISODES	121
COLLIDED FRAMES	46330
# TRIALS TO RESOLVE (AVG)	3.84
# OF DEFERRALS (AVG)	1830
DEFERRAL DELAY (MS) -(AVG)	247.00
DEFERRAL QUEUE SIZE (FRAMES)	0.04
MULTIPLE COLLISION EPISODES	114

4800 POLLING NO CONTROL CHANNEL

INPUT BUFFER USE BY NODE

REPLICATION 1 FROM 1000.0 TO 11150.0 SECONDS

	Packets accepted	Packets blocked	Average Buffer use (bytes)	STD DEV	MAXIMUM
SHIP1	16308	0	0	0	296
SHIP2	1745	0	0	0	296
SHIP3	2339	0	0	0	296
SHIP4	1201	0	0	0	296
SHIP5	2756	0	0	0	296
SHIP6	802	0	0	0	296
SHIP7	3001	0	0	0	296
SHIP8	1729	0	0	0	300
SHIP9	1577	0	0	0	296
SHIP10	1178	0	0	0	296

OUTPUT BUFFER USE BY NODE

	Packets accepted	Packets blocked	Average Buffer use (bytes)	STD DEV	MAXIMUM
SHIP1	16308	0	1453	1610	9496
SHIP2	1737	0	157	576	4736
SHIP3	2331	0	393	877	4736
SHIP4	1201	0	127	517	4736
SHIP5	2740	0	912	2069	7104
SHIP6	794	0	543	990	2392
SHIP7	2993	0	1440	2128	7128
SHIP8	1721	0	174	595	4736
SHIP9	1577	0	122	492	2392
SHIP10	1178	0	106	459	2392

RECEIVED MESSAGE COUNTS 4800 POLLING NO CONTROL CHANNEL

RECEIVER	*COUNT*
SHIP 1	5
SHIP 2	6
SHIP 3	4
SHIP 4	2
SHIP 5	7
SHIP 6	2
SHIP 7	5
SHIP 8	5
SHIP 9	5
SHIP 10	3

Total received: 44

LINK DELAYS AND UTILIZATION 4800 POLLING NO CONTROL CHANNEL

LINK	Delivered frames	Resent Frames	Average Delay	Maximum Delay	Utilization %
HF Packet 4800 Polling	18559	2	460.893	1024.533	84.05

4800 POLLING WITH CONTROL CHANNEL

INPUT BUFFER USE BY NODE

REPLICATION 1 FROM 1000.0 TO 11150.0 SECONDS

	Packets accepted	Packets blocked	Average Buffer use (bytes)	STD DEV	MAXIMUM
SHIP1	16308	0	0	0	296
SHIP2	1745	0	0	0	296
SHIP3	2339	0	0	0	296
SHIP4	1201	0	0	0	296
SHIP5	2756	0	0	0	296
SHIP6	802	0	0	0	296
SHIP7	3001	0	0	0	296
SHIP8	1729	0	0	0	300
SHIP9	1577	0	0	0	296
SHIP10	1178	0	0	0	296

OUTPUT BUFFER USE BY NODE

	Packets accepted	Packets blocked	Average Buffer use (bytes)	STD DEV	MAXIMUM
SHIP1	16308	0	1453	1610	9496
SHIP2	1737	0	157	576	4736
SHIP3	2331	0	393	877	4736
SHIP4	1201	0	127	517	4736
SHIP5	2740	0	912	2069	7104
SHIP6	794	0	543	990	2392
SHIP7	2993	0	1440	2128	7128
SHIP8	1721	0	174	595	4736
SHIP9	1577	0	122	492	2392
SHIP10	1178	0	106	459	2392

RECEIVED MESSAGE COUNTS 4800 POLLING WITH CONTROL CHANNEL

RECEIVER	*COUNT*
SHIP 1	5
SHIP 2	6
SHIP 3	4
SHIP 4	2
SHIP 5	7
SHIP 6	2
SHIP 7	5
SHIP 8	5
SHIP 9	5
SHIP 10	3

Total received: 44

LINK DELAYS AND UTILIZATION 4800 POLLING WITH CONTROL CHANNEL

LINK	Delivered frames	Resent Frames	Average Delay	Maximum Delay	Utilization %
HF Packet 4800 Data	9014	1	457.573	1024.533	40.53
HF Packet 4800 Polling Control	9545	1	464.029	1024.533	43.52

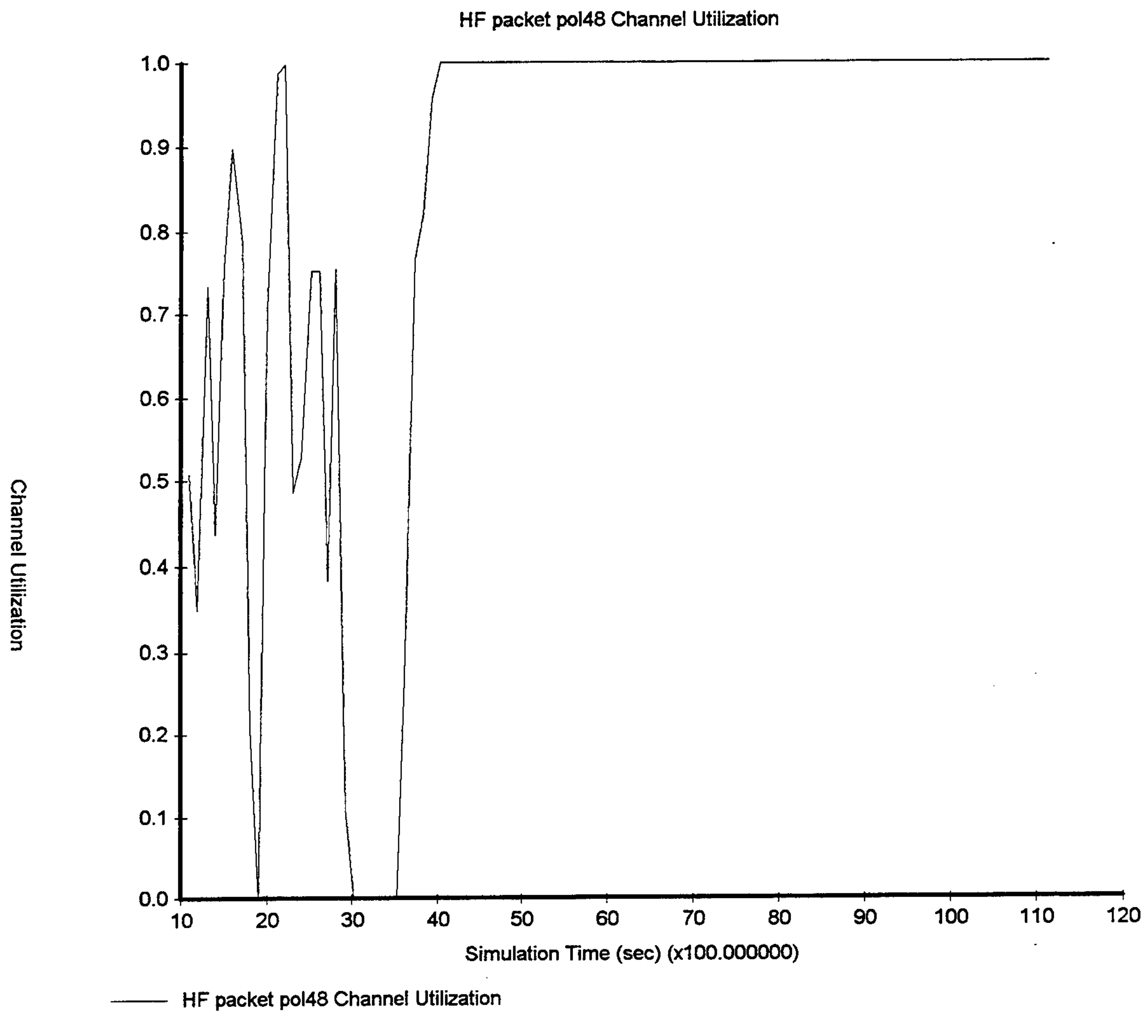
The following Table summarizes the above pages:

	4800 CSMA	***4800 Polling-no con***	***4800 Polling-w/con***	***9600 CSMA***
Total message count	12	44	44	16
User frames delivered	4607	18559	9014	6720
Average transmission delay	781.844 msec	460.893 msec	143.369	331.140
Channel utilization	84.95%	84.05%	40.53%	69.30%
Collided frames %	1000%	na	na	689%

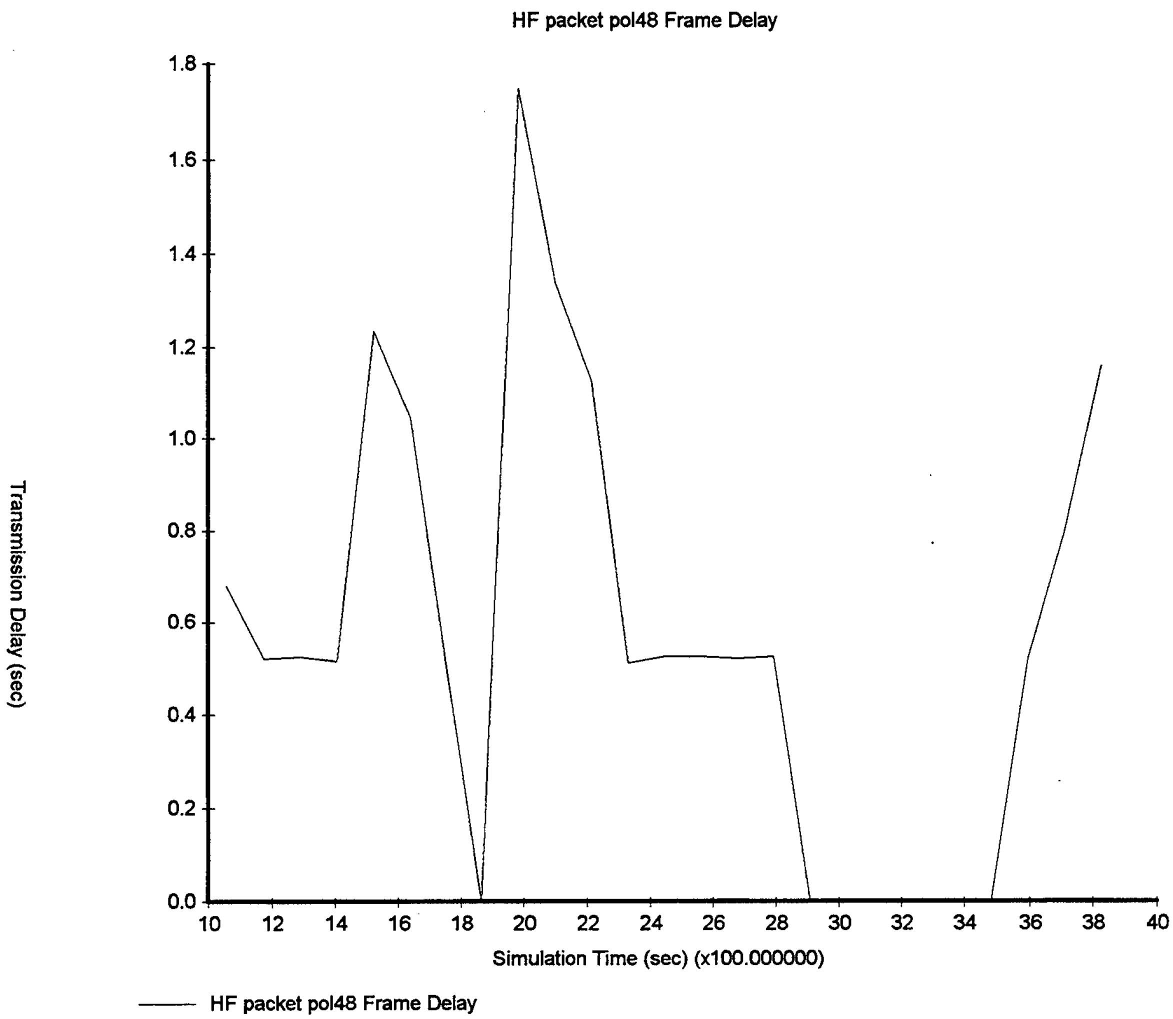
Table 6. Simulation results

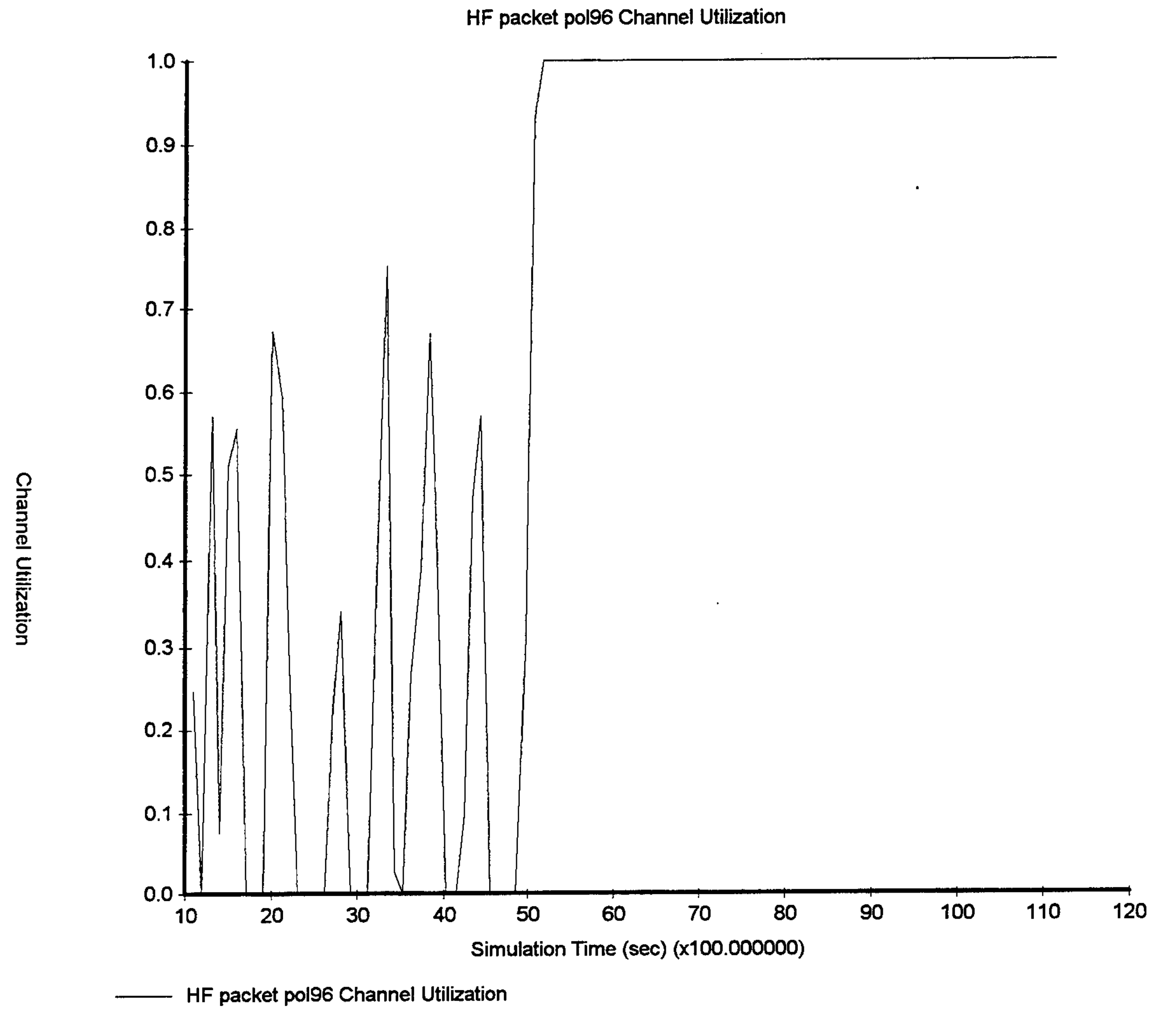
The fact that we observe in the CSMA a high percentage of collided frames is explained by the saturation of the link during the simulation. The simulation stopped after the 3600 sec in the CSMA 4800bps case and after the 4800sec in the 9600bps case.

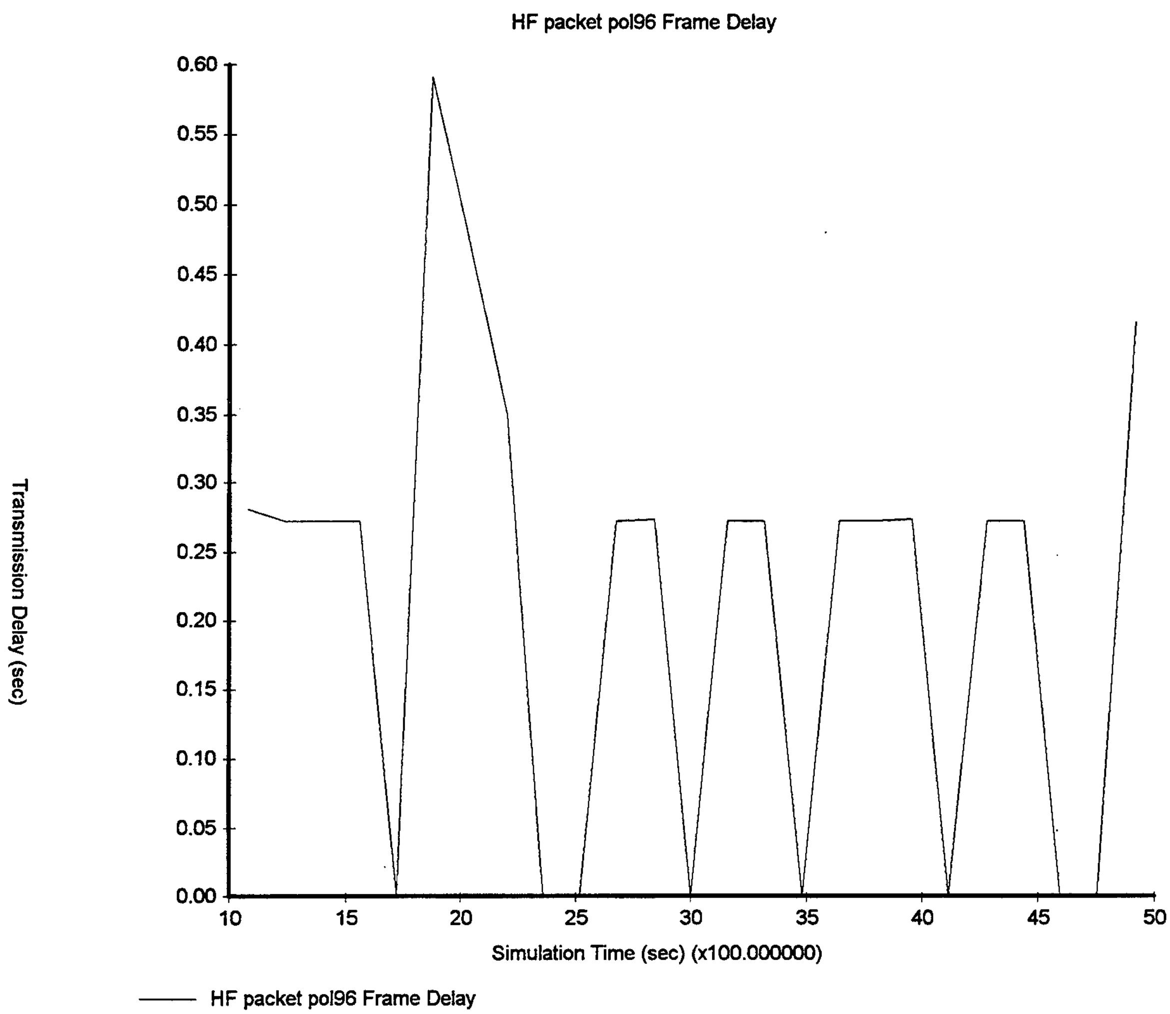
For the 4800bps case, if we assign the 84.95% utilization into two periods of x% for 3600 sec and 100% for 7500 sec, we establish a channel utilization of 54.75% until the 3600 sec when the channel was saturated. Similarly, if we assign the 69.30% utilization for the 9600bps case into two periods of x% for 4800 sec and 100% for 6350 sec we obtain a channel utilization of 28.68%. The following six graphs represent measured channel utilization and frame delays for each network configuration. Notice the sharp increase in channel utilization for the 4800bps and 9600bps CSMA configuration.

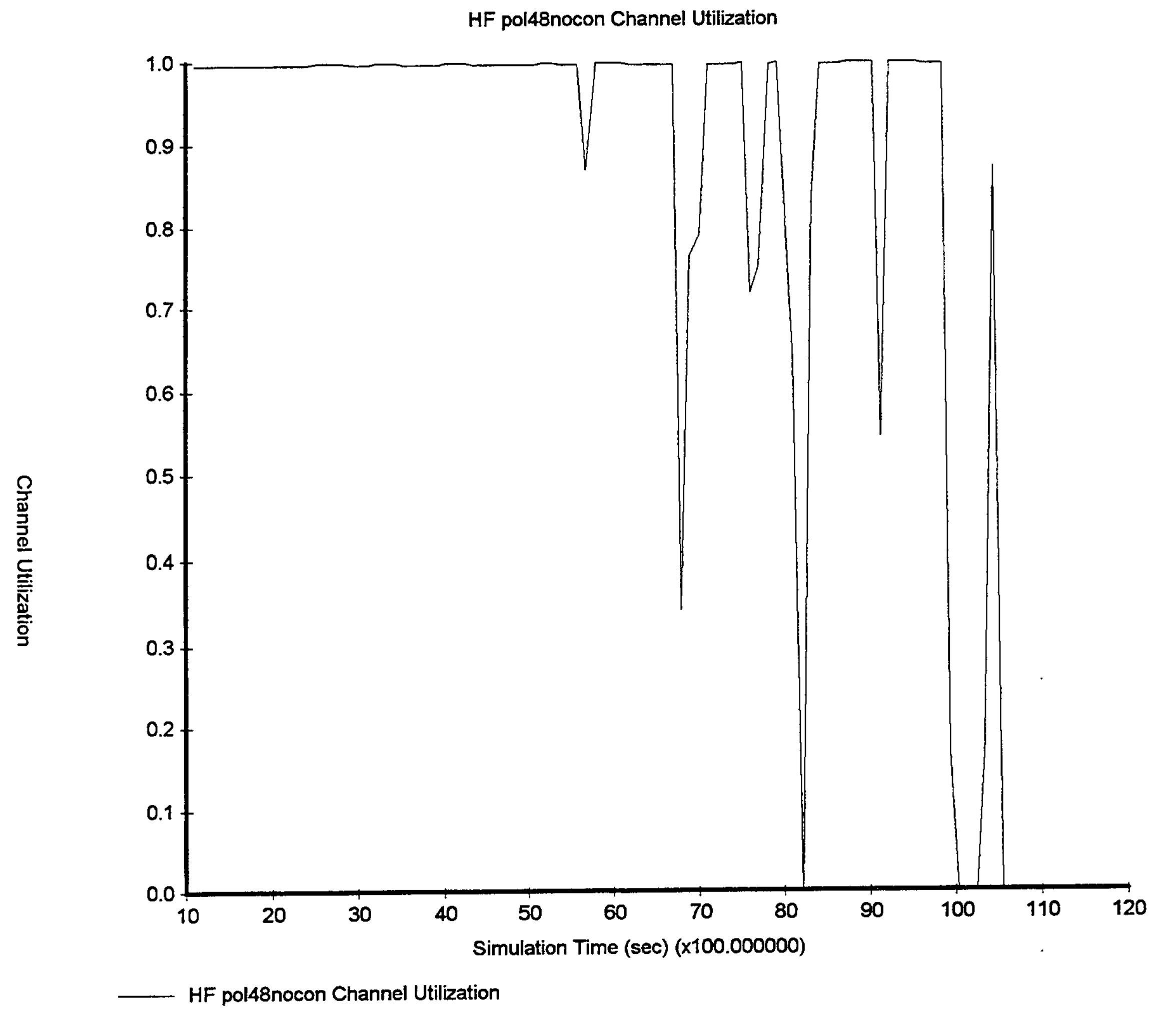


HF packet pol48 Channel Utilization
Channel Utilization
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
10
20
30
40
50
60
70
80
90
100
110
120
Simulation Time (sec) (x100.000000)
HF packet pol48 Channel Utilization

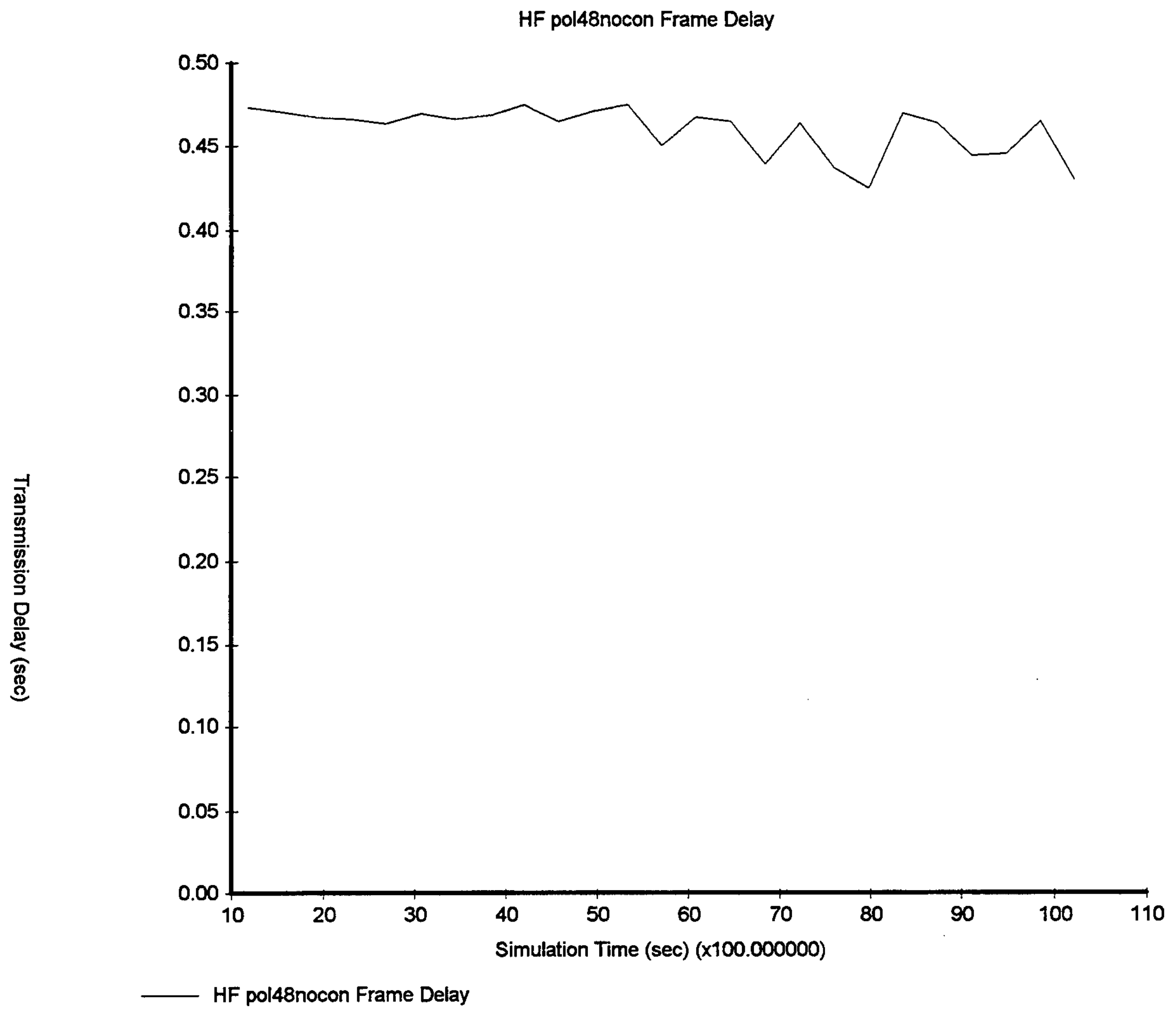

HF packet pol48 Frame Delay
Transmission Delay (sec)
1.8
1.6
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0.0
10
12
14
16
18
20
22
24
26
28
30
32
34
36
38
40
Simulation Time (sec) (x100.000000)
HF packet pol48 Frame Delay


HF packet pol96 Channel Utilization
Channel Utilization
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
10
20
30
40
50
60
70
80
90
100
110
120
Simulation Time (sec) (x100.000000)
HF packet pol96 Channel Utilization

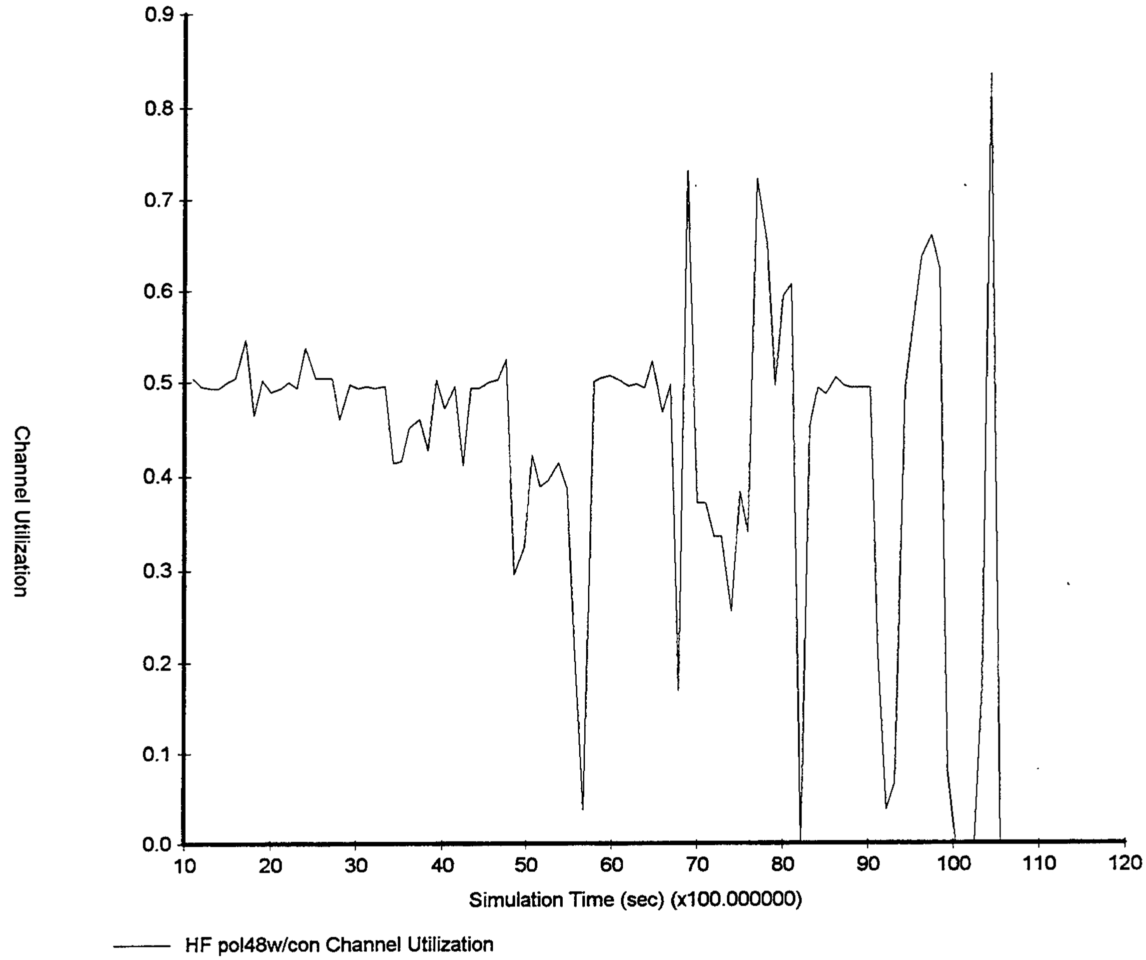

HF packet pol96 Frame Delay
Transmission Delay (sec)
0.60
0.55
0.50
0.45
0.40
0.35
0.30
0.25
0.20
0.15
0.10
0.05
0.00
10
15
20
25
30
35
40
45
50
Simulation Time (sec) (x100.000000)
HF packet pol96 Frame Delay

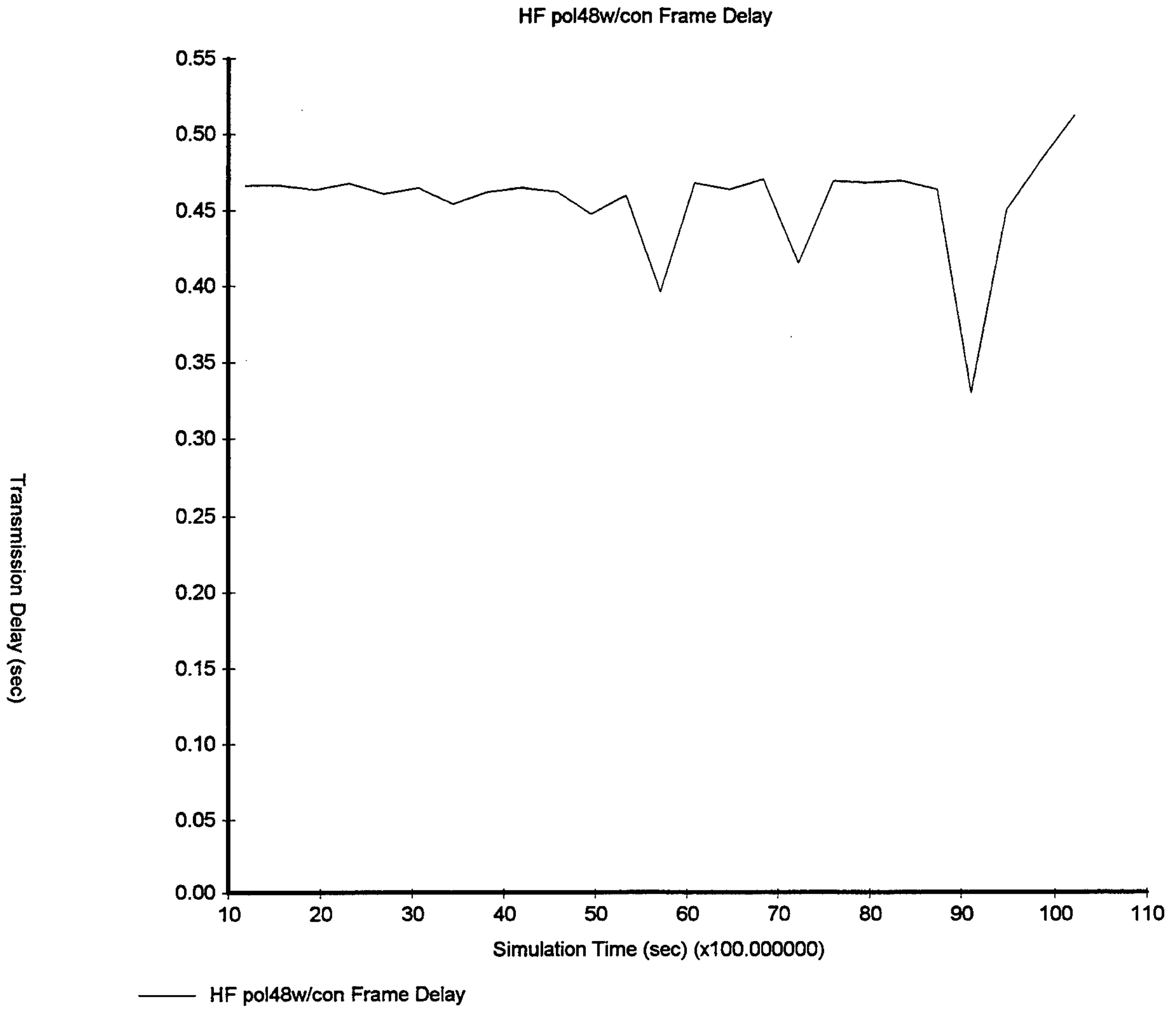


HF pol48nocon Channel Utilization
Channel Utilization
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
10
20
30
40
50
60
70
80
90
100
110
120
Simulation Time (sec) (x100.000000)
HF pol48nocon Channel Utilization

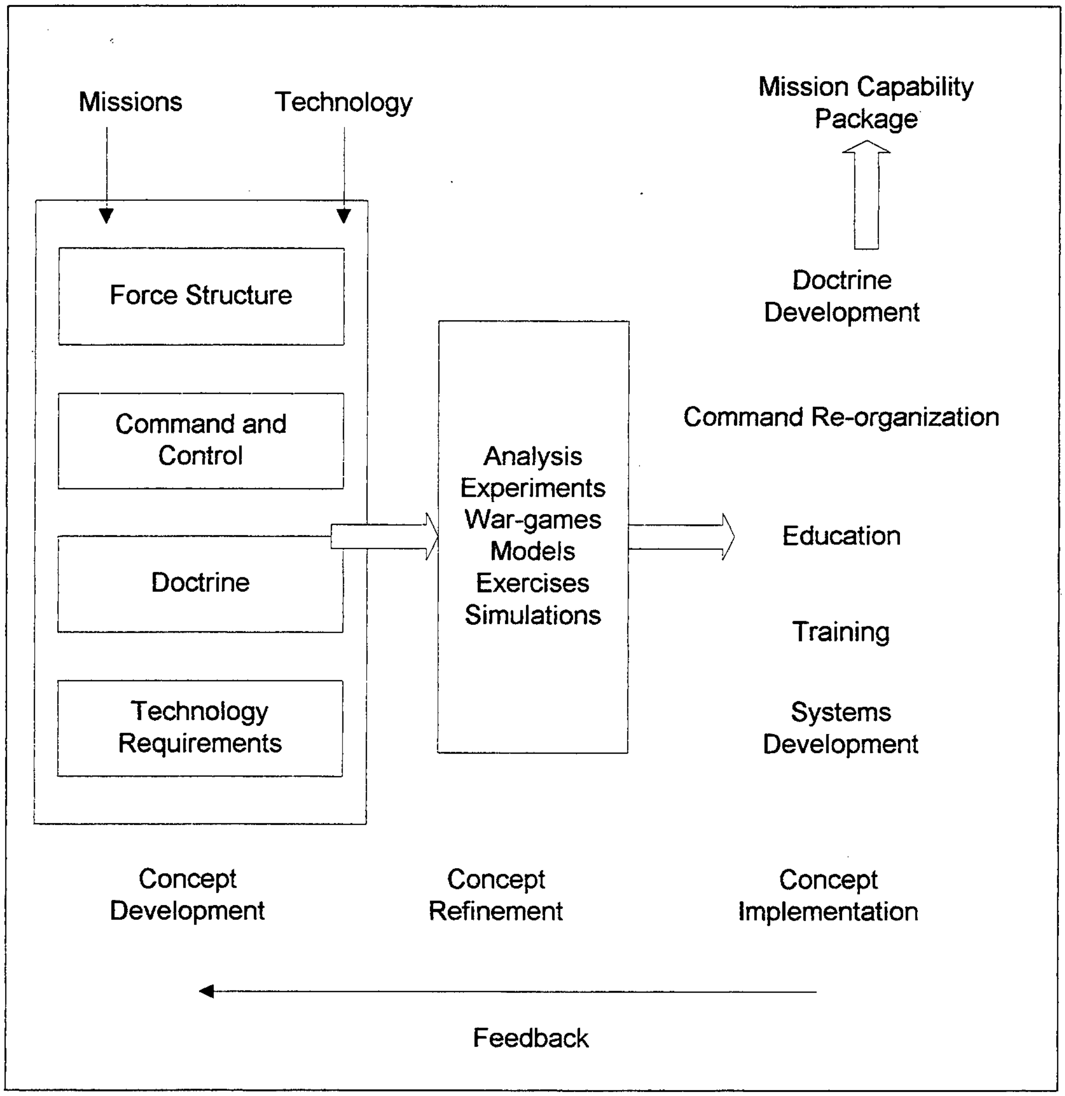

HF pol48nocon Frame Delay
Transmission Delay (sec)
0.50
0.45
0.40
0.35
0.30
0.25
0.20
0.15
0.10
0.05
0.00
10
20
30
40
50
60
70
80
90
100
110
Simulation Time (sec) (x100.000000)
HF pol48nocon Frame Delay

HF pol48w/con Channel Utilization




HF pol48w/con Frame Delay
Transmission Delay (sec)
0.55
0.50
0.45
0.40
0.35
0.30
0.25
0.20
0.15
0.10
0.05
0.00
10
20
30
40
50
60
70
80
90
100
110
Simulation Time (sec) (x100.000000)
HF pol48w/con Frame Delay

APPENDIX D. MISSION CAPABILITY PACKAGES



Mission Capability Packages. From Johnson and Libicki, 1995

LIST OF REFERENCES

Adamson, B. *Tactical Radio Frequency Communication Requirements for IPng.* RFC 1677, NRL, August 1994

Alanko Timo et al. *Measured Performance of Data Transmission Over Cellular Telephone Networks.* Report C-1994-53, University of Helsinki, Helsinki, 1994

Alberts, David S. *Unintended Consequences of Information Warfare.* NDU Press, Washington, DC, 1996

Blommers, John. *Practical Planning for Network Growth.* Prentice Hall PTR, Upper Saddle River, New Jersey, 1996

Bradner, Scott O., Mankin Allison (eds.) *IPng Internet Protocol Next Generation.* Addison-Wesley, Reading, MA, 1996

Buddenberg Rex et al. *SeaNet: Extending the Internet to the Oceanographic Research Fleet.* Unpublished pre-proposal draft, October, 1996

Buddenberg, Rex, A., IS4502 *Telecommunications Networks Class Notes,* http://dubhe.cc.nps.navy.mil/~budden/lecture.notes/net-centric.html, 1993

Buddenberg, Rex, A., *Ship-Shore Packet Switched Communications System.* Thesis, Naval Postgraduate School, Monterey, CA, June, 1986

Burn Janice, Caldwell Eveline. *Management of Information Systems Technology,* Van Nostrand Reinhold, NY, 1990

CACI, *Comnet III User's Manual. Planning for Network Managers.* CACI, Washington, DC, 1996

Cohen, Eliot, A. *A Revolution in Warfare.* Foreign Affairs Volume 75, No. 2, March/April 1996, pp.37-54

Conard, James W. (ed.) *Handbook of Communications Systems Management.* Auerbach Publications, Boston, MA, 1994

Danielson, Terry. *Navy Implementation of a Battle Force E-mail System Operating Protocol.* NCCOSC RDTE DIV Code 846, San Diego, CA, 1996

Danielson, Terry. *Battle Force Electronic Mail.* Naval Command, Control and Ocean Surveillance Center, San Diego, CA, 1996

DARPA Packet radio research overview at SeaNet web page at the Naval Postgraduate School. http://dubhe.cc.nps.navy.mil/~seanet/packetradio.htm (January 1997)
DREO Adaptive, Packet Switched HF-Terminal. Located at web site: http://www.dreo.dnd.ca/pages/comms/dc002.htm (January 1997)

Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations, Joint Pub 6-0, Joint Chiefs of Staff, May 1995

Grenier, Ray and Metes, George *Enterprise Networking. Working Together Apart.* Digital Equipment Corporation, 1992

Hegering, Heinz-Gerd and Abeck, Sebastian *Integrated Network and System Management,* Addison-Wesley, NY, 1994

Henderson, Christopher B. *The Warfighters' Link to Information.* Thesis, Naval Postgraduate School, Monterey, CA, June 1996

Hoffman, Gerald M. *The Technology Payoff. How to Profit with Empowered Workers in the Information Age.* Irwin, NY, 1994

Johnson, Stuart and Libicki, Martin. *Dominant Battlespace Awareness.* NDU Press, http://198.80.36.91/ndu/inss/books/dbk/dbk1.html, 1995

Kahin, Brian and Wilson, Ernest (eds.) *National Information Infrastructure Initiatives. Vision and Policy Design.* MIT Press, Cambridge, MA, 1997

Khosrowpour, Mehdi (ed.) *Information Technology and Organizations: Challenges of New Technologies.* Idea Group Publishing, Harrisburg, PA, 1994

Kim John, C., Muehldorf, Eugen I. *Naval Shipboard Communications Systems* Prentice Hall, Englewood Cliffs, New Jersey , 1995

Lippis, Nick. *The Client is the Network.* Data Communications March 1997, pp.23-24

Maslin, Nicholas. *HF Communications. A Systems Approach.* Plenum Press, NY, 1987

Scheider, Carl. *Information Architecture Strategy.* The Information Architects' Cooperative (TiAC), 1996

Spewak, Steven H., Hill, Steven C. *Enterprise Architecture Planning.* QED Publishing Group, Wellesley, MA, 1993

Stallings, William. *Network and Internetwork Security. Principles and Practice.* Prentice Hall, Englewood Cliffs, New Jersey, 1995

Tactical Packet Radio Project. http://www.itr.unisa.edu.au/dcrc/packet.html, 1996

Tanenbaum, Andrew S. *Computer Networks.* Prentice Hall, Upper Saddle River, New Jersey, 1996

Turner, Darren L. *Command and Control Architecture for Multi-National Operations.* Thesis, Naval Postgraduate School, Monterey, CA, March 1992

Wolstenholme et al. *The Evaluation of MIS. A Dynamic and Holistic Approach.* John Wiley and Sons, NY, 1993

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center..2
   8725 John J. Kingman Road., Ste 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library...2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, CA 93943-5101

3. LT. Panagiotis Lymberis..4
   Prokopi Katsouli 11
   N. Iraklio, Athens 14121 Greece

4. CDR John Allan USCG..1
   Commandant (G-AIR/NDS)
   US Coast Guard
   Washington, DC 20593

5. Mr. Gordon Shillito...1
   1015 Chestnut Ridge Dr.
   Martinsburg, West Virginia 25401